The Panoptic Principle:

Privacy and Surveillance in the Public Library as Evidenced in the Acceptable Use Policy

Elaine Robinson

Submitted in partial fulfilment for the degree of Doctor of Philosophy

Department of Computing and Information Sciences

University of Strathclyde

Submitted 2018

Declaration

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree

.

Signed:

Date:

Abstract

Facilitating access to the Internet is an important part of the public library profession. Part of managing this access relies on the acceptable use policy, an agreement between the library and the user regarding the conditions of access. This study analysed acceptable use policies in UK public libraries to ascertain whether they exhibit Michel Foucault's panoptic principle, a metaphor for surveillance derived from Jeremy Bentham's Panopticon, an institutional inspection building. The policies were also analysed as to how they encourage and discourage information access through surveillance, filtering, and demonstration of the ethical principles of the profession. The effectiveness of balancing the caring and controlling elements of public access was also analysed, influenced by David Lyon's theories regarding caring and controlling aspects of surveillance.

The study analysed 205 of the 206 acceptable use polices across UK public library authorities. The policies and authorship details were collected via Internet searching and freedom of information request. Readability testing was then used to establish the difficulty of the documents. After this, qualitative content analysis was used to investigate the language of the policies.

The acceptable use policies were found to be too difficult to understand easily. They exhibited aspects of the panoptic principle, they encouraged access by reflecting ethical principles and they discouraged access due to the inconsistent application and description of filtering software. The policies were varied in tone and content, demonstrating both caring and controlling aspects of public access.

The findings suggest a single acceptable use policy would be recommended. This way access would be consistent through the country. It is also recommended that the policy should have more clarity regarding aspects such as filtering and what the aims of the service are. The findings of the study were then used to create a model acceptable use policy that could be used and disseminated.

Acknowledgements

I would like to thank my supervisor, David McMenemy, for the opportunity to conduct this research and for his guidance and support throughout the research process.

I would also like to thank my partner, Muv, for his love and encouragement.

The funding provided by the Economic and Social Research Council through the Scottish Graduate School of Social Science's Information Science pathway is gratefully acknowledged.

Contents

List of Tables

List of Figures

1 Introduction

The purpose of this research was to explore panopticism and acceptable use policies in UK public libraries. To achieve this, firstly the literature was surveyed. This was a combination of surveillance and panopticism research, research on ethics, and ethics in librarianship, and access management in libraries, including acceptable use policies, filtering, and surveillance.

Acceptable use policies were requested from the 206 public library authorities in the UK. These were then subjected to readability testing and qualitative content analysis. The literature review was used to inform the themes, to be used in the qualitative content analysis. The findings from these then informed the creation of a new model acceptable use policy which is suitable for public library use.

The remainder of this chapter provides an overview of the study as it was carried out. Firstly, an overview of the background and reasoning for this research. Then, the research goals and methods will be described. Finally, this chapter will conclude with a summary of the succeeding chapters.

1.1 Background and motivation for this research

The motivation and impetus for this research comes from an earlier study in 2013 for the researcher's dissertation project as part of the Master of Science degree in Information and Library Studies at the University of Strathclyde. The researcher used discourse analysis to study public library acceptable use policies from a random selection of 30 policies made available through Internet searching. Surveillance was found to be heavily prevalent in the acceptable use policies, alongside information on what is regarded as misuse of the facilities, and a heavy focus on the topic of banning as a consequence of misuse. As well as this, there were noted uses of vague statements to describe what was perceived as misuse of the facilities. The surveillance as described in the acceptable use policies was both coercive, used for disciplinary measures, to weed out and spot potential abuses of the system and bad behaviour, and also protective, used to monitor the safety of patrons, with children being a particular focus. The documents varied in length, tone, and topic. Some of

the acceptable use policies were only a page long, whereas others ran over half a dozen pages. This disparity in length, along with differences in tone prompted the researcher's interest as to what other acceptable use polices around the country would contain, and how they differed from each other or were similar to one another.

Although there has been some research into acceptable use policies and access management in libraries (such as surveys by Willson and Oulton (2001), unobtrusive testing by Brown and McMenemy (2013), the Managing Access to the Internet in Public Libraries project (Cooke et al., 2014; Spacey et al., 2014; Spacey et al., 2015), and Gallagher et al.'s discourse analysis of acceptable use policies in Scotland (2015)) actual research into acceptable use policy content was relatively low, especially in regards to a nationwide study. The importance of such a document, one that acts as an agreement between the library user and the library service, provides a fruitful area of research. The public library acceptable use policy in particular is an important document – for some library visitors, the public library is their only access to the Internet and such a document is a major part of managing that access.

The researcher decided to analyse the policies herself, rather than investigate the ways in which patrons understand the policies. This was due to the importance attached to such documents, and the lack of attention given to such documents. The acceptable use policy is a key document that connects the library user to the use of the library computers and Internet. This document has not always been given the attention it deserves, indeed studies such as Poulter et al.'s (2009) research of public library IT access demonstrates the lack of interest in such documents. The lack of research in this area, combined with the importance of such a document, and the lack of standardisation made apparent in the pilot study by the researcher made this to be an important area of study. Such a document should convey the mission of the public library, as well as demonstrate how the public library provides its services. How it conveys different points in the acceptable use policy such as surveillance, filtering, and information access can potentially have an encouraging or discouraging effect

on the library patron. Analysing these documents from across the country will demonstrate how public ICT access is provided across the UK, giving a deeper understanding of public library ICT facility access in general.

The panoptic principle comes from Michel Foucault's interpretation of the Panopticon, an institutional building designed for maximum surveillance by social reformer and philosopher Jeremy Bentham, in the late 18th century. A building comprised of single cells and a looming watch tower would make the surveillance subjects start to self-monitor and modify their behaviour as if they were being watched at all times, regardless of whether this was actually the case. Foucault suggests that panopticism can be witnessed in many aspects of modern society, including schools and hospitals, as a way to control and discipline the population. The panoptic principle has since become a major metaphor in surveillance studies (e.g. Wood, 2003; De Saulles and Horner, 2011; Bakir, 2015), where the idea of subjects practicing self-surveillance, under the threat of omnipresent watchers pervades various aspects of daily life.

Despite the panoptic metaphor's popularity in modern surveillance studies, research into panopticism in the public library is relatively rare. Most studies are restricted to historical research of libraries (such as Hewitt (2000), and Black (2001; 2005)). A recent study into panopticism in modern public libraries was Gallagher et al.'s discourse analysis of public library acceptable use policies in Scotland (2015). The acceptable use policy should encourage access to information and freedom of expression so analysing to find if the panoptic principle does exist in public library acceptable use policies could provide revealing insights into how access is provided and discussed by the library service.

1.2 Research design

The research questions for this study were:

- RQ1 In what ways does the public library acceptable use policy document reflect the panoptic principle?

- RQ2 How does the public library acceptable use policy encourage and discourage access to information and freedom of expression through surveillance, filtering, and commitment to ethical principles?
- RQ3 How effectively does the acceptable use policy balance the care and control elements of public access?

1.3 Methods

This study used a mixed methods approach, utilising freedom of information requests for data collection, alongside readability testing, and qualitative content analysis. The research used an explanatory sequential design whereby the quantitative aspects of the research, the readability testing, was expanded upon by the qualitative findings of the content analysis (Bryman, 2012). There will be a short breakdown of the data collection and analysis methods here, with fuller details on the design appearing in the relevant methods chapter.

1.3.1 Data collection: freedom of information request

To collect the acceptable use policies, a combination of Internet searching and freedom of information requests were used. Freedom of information requests are an invaluable means of collecting documents that are held by local authorities, and are helpful for gathering large volumes of data (Savage and Hyde, 2014: 308-309). A freedom of information request was sent to all 206 public library authorities in the UK. Some of the requests were for both a copy of the acceptable use policy and to ask who created it, whilst some asked for authorship details only. The research garnered 205 out of a possible 206 policies, a return rate of 99.5%.

1.3.2 Readability testing

When the acceptable use policies were gathered, the documents were put through readability testing via the readability calculating website: www.readable.io (previously www.readability-score.com). The four readability tests chosen were:

- Flesch Reading Ease

- Gunning Fog Index
- SMOG (Simple Measure of Gobbledegook) Grade
- Coleman-Liau Index

These tests were chosen because of their popularity and reliability (Wilson et al., 1997; Hedman, 2008; Fitzsimmons et al., 2010; Kondilis et al., 2010; Rudd, 2010; Luk and Aslani, 2011; Svider et al., 2013; Wang et al., 2013; Best et al., 2015; Hamnes et al., 2016; Kugar et al., 2017). These tests use a combination of polysyllabic word count, sentence length, and character count to generate a grade or score that determines the difficulty of a piece of writing.

1.3.3 Qualitative content analysis

After the readability testing, qualitative content analysis was used to study the language of the acceptable use policies. Qualitative content analysis was chosen as it allows for the quantitative aspects of content analysis, such as frequency counts, whilst also allowing the interpretative approach that comes with qualitative analysis (Gbrich, 2007). Qualitative content analysis also allows for both manifest and latent aspects of language to be explored (Hsieh and Shannon, 2005). Qualitative analysis is accepting of the constitutive nature of nature of language, allowing for an interpretative approach and, like discourse analysis, the meaning of such language is “not immutable, but that it is constructed in the context of the questions asked of it” (Williamson et al., 2018: 461). Analysis can be inductively or deductively driven (Hsieh and Shannon, 2005; Elo and Kyngäs, 2008). It allows for unobtrusive analysis of that data, and is ideal for studying written communication (Vaismoradi, 2013). The acceptable use policies were imported to the NVivo software suite to assist analysis.

1.3.4 Pilot study

Due to the large volume of documents to be analysed (potentially 206), it was decided that a pilot study of the qualitative content analysis would be conducted in order to test out the

themes formulated from the literature review. A dataset of 30 acceptable use policies already held by the researcher was used for this.

1.4 Chapter outlines

The rest of this work will be structured as follows.

The literature review comprises two separate chapters. The first will give an overview of the context of access management in libraries, such as filtering, surveillance, and the acceptable use policy.

The second literature review chapter will take a thematic approach, providing a theoretical framework for the research. This chapter will introduce Jeremy Bentham's Panopticon design and its subsequent history. This then goes on to look at Foucault's use of the panoptic metaphor and how it relates to a disciplinary society, and will look at how the Panopticon has been used to inform research. There will then be an overview of surveillance studies in general. After this, there will be an overview of ethics, and ethical considerations in the library.

The next chapter discusses the methods used in this study. The approach for this study was an explanatory sequential model, using mixed methods, both quantitative and qualitative. This study used freedom of information requests to collect the data, alongside readability testing and qualitative content analysis to analyse the data. A description of, and the reasoning behind these methods will be described in more depth in this chapter, and the coding framework is also provided as Appendix 1. The limitations of the methods will also be discussed here.

Chapter 5 will be dedicated to the quantitative findings and discussions of the study. This chapter will provide the results of the study, including the freedom of information requests, and readability testing.

Chapter 6 will present findings from the qualitative content analysis whilst also discussing the findings in depth, along with how the findings reflect and contrast to previous research.

Chapter 7 will present a model acceptable use policy, which has been made by synthesising the findings from this study alongside best practice as informed by the literature review. The full model policy appears in Appendix 2.

Chapter 8 will be a concluding chapter. It will answer the research questions posed by the study, outline the contributions to knowledge this study has made, make recommendations informed by the findings of this study, and will outline possible future research areas.

2 Literature review: access management context

2.1 Introduction

This chapter gives an overview of Internet access management in the library sector. Access management in libraries includes surveillance, Internet filtering, and acceptable use policies (AUPs). The different types of surveillance in libraries will be described, why surveillance is used in the library, and the research context on how surveillance is carried out and impacts the library service. There will be an overview of Internet filtering, and discussion of arguments for and against using such software. The chapter will also give an overview of the AUP, what it should contain, and its importance to access management and the potential pitfalls of how it is written and deployed.

2.2 Access management

Managing access to the Internet is an important aspect of the public library. The library is not in control of the Internet, and thus having certain policies and standards in place is particularly important, both for the library and its user base (ALA, 2007b; Pautz, 2013; McMenemy, 2014). Computer and Internet access needs to be managed in the public library for various reasons such as illegal use of the search facilities (McMenemy and Burton, 2005) and to help protect patrons against cybercrime which is a growing problem (Europol, 2013). Stewart (2000) notes that in corporations, those suffering from bad publicity due to employee misuse will lose business; likewise, a library could share the same fate. Managing access to the Internet is also important in the event of possible liability issues (McMenemy and Burton, 2005). As well as this, libraries are government-funded with several different stakeholder groups to be accountable for, and thus will have an expectation of access management (Sturges, 2002; McMenemy 2016). Environments that are seen to not be managed could put off current and potential service users (Morris et al., 2013).

Although access management is important for the library, some aspects of access management also come into conflict with the ethical principles of librarianship. Technology such as filtering software and electronic surveillance can serve to undermine both the

patron's freedom of access and privacy. However, in order to protect patrons from potentially offensive content, and to be socially responsible in their community, the public library may feel certain acts of access management are necessary to best serve their users: the library must allow freedom of expression, whilst also making the library environment a safe place for those who may be disturbed by certain types of content (Young, 1997). The public library staff have to balance the needs of those individuals the library serves whilst also being mindful of the fact that the library is a publicly funded institution: "On the one hand, libraries must respect the principle of intellectual freedom as their institutional mission... On the other hand, library functions are human targeted, and are morally responsible to their users. A librarian should respect both public morals and human life" (Trushina, 2004: 418). Indeed, one of the Chartered Institute of Information and Library Professionals (CILIP)'s ethical principles is "Concern for the public good in all professional matters, including respect for diversity within society, and the promoting of equal opportunities and human rights" (CILIP, 2013). This includes freedom of expression and individual privacy, but the notion of concern for the public good also includes what is best for the community as a whole. Below are some aspects of access management, and possible ethical issues arising from such measures.

2.2.1 Methods of access management

2.2.1.1 Filtering

Filtering software attempts to block or control content on the Internet that a user can access using a set of pre-defined criteria. In the library this is usually to prevent patrons from accessing sites that may be objectionable to fellow users (such as pornography) or that may be bandwidth intensive (such as websites dedicated to playing games). Early filtering systems scanned web pages for specific words and blocked accordingly, this then expanded to include website databases, with website addresses being checked against a list of websites (Stewart, 2000). Filtering software now uses a combination of methods, including IP addresses, stopwords, and repositories of domain names (Shirazi, 2012). Certain words or URLs are placed on a blacklist and the filtering software responds accordingly (Aceto and

Pescapé, 2015). Filtering can also be IP-based, particularly in countries with heavy censorship and can be used to block entire subnets (Chaabane et al., 2014: 1).

Filtering is a widely used method of access management. In a study of Internet access management, Willson and Oulton distributed a survey to public libraries regarding different types of controls. 71% of respondents stated that some sort of control was being used on public access computers – employing blocking software and monitoring by visual checks, with 60% using filtering mechanisms, often decided at a county rather than library level (Willson and Oulton, 2000). In 2013, Brown and McMenemy sent freedom of information (FOI) requests to all 32 public library authorities (PLAs) in Scotland. All 31 of the authorities that provided information utilised filtering software (Brown and McMenemy, 2013). The MAIPLE (Managing Access to the Internet in Public Libraries) project's analysis of access management in public libraries across the UK found that 100% of respondents to the project's survey stated that they used filtering software (Cooke et al., 2014). A 2016 study undertaken by volunteers from the Radical Librarians Collective using the Freedom of Information Act found that at least 98% of public libraries filter online content (Payne, 2016).

2.2.1.1.1 Arguments for filtering

The Internet has made it easy to obtain information: "What formerly took some real physical and intellectual effort is now just a few keystrokes away" (Hauptman And Motin, 1994: 8). This information can have both law-abiding and nefarious purposes: instead of having to pore over textbooks, one can simply scroll through a Wikipedia page to learn all there is to know on cordite. Even if a library patron does not want to see any offensive material, that does not mean they will avoid it. Cottrell (1999) notes that searching for even the most mundane of subjects can provide the user with results that may distress or disturb. One of the best – and perhaps worst – things about the World Wide Web is the access to millions upon millions of bits of information, which comes in many different, sometimes rather explicit forms. Some of it may be helpful, but some of it may be unwanted, and possibly offensive. By and large, this type of distress can be easily avoided when searching through the texts

housed on the library shelves. On the Internet however, it is a different story: “In a traditional print setting, a patron would be unlikely to encounter such a result; on the Web, it is not uncommon” (Cottrell, 1999: 110). Libraries have always had a selection process, and it could be argued that filtering is merely an extension of this (Pors, 2001). By using filtering software, the library can make sure that such content is hidden from the patron. In a debate regarding Internet filtering and whether it infringes upon access to information, Auld related a story from a library worker who stated that during the pre-filtered Internet phase in the library, they saw pornography on a near daily basis, whilst after the introduction of filtering pornography had all but disappeared (Auld and Kranich, 2005). In another story, Auld notes that when there are no filters, communities and staff have complained about the content they have to see: “There also had been a grievance by library workers who, according to their union, were being made physically ill by what they were forced to see in the name of intellectual freedom” (Auld and Kranich, 2005: 196). Heok and Luyt (2010) noted that librarians in Singapore felt access management tools such as the ability to block certain URLs reinforced their confidence when managing Internet access. Likewise, the MAIPLE project (Spacey et al., 2014) found that library staff viewed filtering software as an effective method of managing Internet access. Filtering content can also help to reassure patron concerns over accessing content that is illegal (Willson and Oulton, 2000).

Filtering software is also seen as a logical extension of keeping children safe: “The prudent use of Internet filters will ensure the greatest amount of safety and security for children and adults who do not want to be exposed to a side of the Internet that offends them” (Auld and Kranich, 2005: 198). The library is supposed to represent a safe space for the community, and one in which adults and children can feel free to access information. Filtering can help parents feel safe in the knowledge that their child has some protection against the possibility of viewing offensive sites (Helmrich and Howerton, 2011). Przybylski and Nash (2018) note that filtering software is widely used by caregivers to protect children from accessing sexual materials. Added to this, the library should serve the community, thus it makes sense for the

library to use filters if the community wishes it (Auld and Kranich, 2005). The public library is also accountable to its various stakeholders such as its user base (McMenemy, 2016). The MAIPLE project found that both library users and staff to be broadly in support of filtering; some staff members voiced concern over censorship, but they cited the protection of children as being the main concern (Cooke et al., 2014). Infopeople note that after the enactment of the Children's Internet Protection Act (CIPA) (legislation in the US requiring libraries to use filtering software to receive funding), those libraries that installed filters found that they received less complaints (Infopeople, n.d.). Libraries can also retain certain areas to be children-only, allowing for adults to have unfiltered access (Skaggs, 2002).

2.2.1.1.2 Arguments against filtering

One of the main arguments against filtering is that by denying patrons access to content, it is effectively a form of censorship: “It is an acceptable form of censorship for many organisations, but it is in the raw definition of the word, censorship” (McMenemy and Burton, 2005: 22). Such practice goes against fundamental library ethics (Spacey et al., 2015). Censorship can be detrimental in particular to those who may not otherwise be able to access the Internet. Debating Internet filtering in US public libraries, Kranich states: “Unfortunately, when many libraries that are committed to providing equitable access and bridging the digital divide rely on federal funds, they are required to use filters that block numerous sites available to those fortunate enough to have access at home, thereby relegating their neediest citizens to second-class Internet users” (Auld and Kranich, 2005: 199).

The argument that filtering is censorship is exacerbated by both its unreliability and the overreliance on its perceived reliability. Filtering is not an infallible method of blocking content (Cooke 2006; Scales, 2009; Shirazi, 2012). Filters can both underblock or overblock material (Stewart, 2000; Skaggs, 2002; Wyatt, 2006; Pautz, 2013; May, 2014; ALA, 2015). Underblocking is when the filtering software fails to block websites that should not get through the filters, and overblocking websites means that the filtering software is blocking

websites that should get through (Resnick et al., 2004). Filters have been found to block the Bible and plays by Shakespeare, as well as World War II history websites and websites providing information on breast cancer and sexuality (Sobel, 2004; Houghton-Jan, 2008; Holt, 2011). If a filter relies on keywords, it can falter when it is confronted with the nuances of language (Minow, 1997). Filters have been found to block more information incorrectly than they do block information correctly (Jaeger and Bertot., 2011: 250. See also: Jaegar et al., 2005). This lack of nuance has made filtering controversial (Poulter, 2005). Despite technology having been much improved, the lack of a human touch still renders a lot of filtering software ineffective:

“By 2001, some filter manufacturers said that they had corrected the problem of overblocking, and that instead of keywords, they were now using “artificial intelligence.” But no matter how impressive-sounding the terminology, the fact remains that all filtering depends on mechanical searches to identify potentially inappropriate sites” (Heins, 2006).

Although filtering software is a popular option for guardians, Przybylski and Nash (2018) note the efficacy of filtering is poorly understood. If filtering is relied upon too heavily as a cure-all, this can backfire upon patrons and the library: the use of filtering software could “create an implied contract with library users that they will not be exposed to illegal or harmful material when using the Internet. In particular parents may believe that their children will not be able to access such material in a library” (Library Association 2000, cited in Willson and Oulton, 2000: 199). The Library Association then goes on to note that this could leave the library service liable due to its limitations (Library Association 2000, cited in Willson and Oulton, 2000). It can lull parents and users into thinking the more offensive areas of the Internet are out of reach, when in fact the protection is not necessarily unmitigated (Pors 2001; Kranich, 2004; Gottschalk, 2007). A study by Przybylski and Nash (2017) using in-home interviews found that despite the use of filtering software, early adolescents were still subjected to aversive online experiences. In a further study it was concluded that the use of

filtering by caregivers in order to shield young people from accessing sexual content online was “entirely ineffective” (Przybylski and Nash, 2018: 409).

Overblocking and underblocking both have their own distinctive problems. Underblocking will potentially cause emotional distress to children and adults alike, if they stumble upon content that they expect to be blocked that is offensive or distressing. Overblocking is problematic because it denies access to lawful content (Spacey et al., 2015). As well as this, it may not be clear to the user what is taking place, depending on how the blocked page is presented (McMenemy, 2008). In libraries, this can be further exacerbated by some libraries not communicating that they use such software. Brown and McMenemy (2013) used FOI requests to survey Scottish PLAs. 31 out of the 32 responded, and all 31 of those that answered stated they did utilise filtering software. However, in their analysis of public library AUPs in Scotland, Gallagher et al. (2015) found that only 26 of the 32 AUPs examined stated explicitly that they used filtering software. If the user was aware of what was happening, they may simply be able to ask the library staff to have a website blocked or unblocked, however in the case of unblocking it is also possible they may not wish to discuss with the library staff that they need access to a website, particularly if the subject is of a sensitive or personal nature (McMenemy, 2008; Spurlin and Garry, 2009; McMenemy et al. 2014). If filtering software is seen to be in place, it can also lead to users self-censoring their searches (Przybylski and Nash, 2017). The problem may also be exacerbated by the difficulty to stop or override some filters (Kranich, 2004; Auld and Kranich, 2005). The decision-making can also be taken out of the librarian’s hands altogether, if filtering is being imposed as a county policy, rather than a local one, as was found in Willson and Oulton’s (2000) survey of public libraries. Surveys sent out by the MAIPLE project found that fewer than 10% of library services give frontline library staff any responsibility to respond to filtering change requests with one service having to completely rely on an outsourced IT company (Spacey et al., 2015).

Some have argued that filtering is merely an extension of the library's already defined role of information selector (Gottschalk 2007). However, as noted by studies such as the MAIPLE project, the decision may be far removed from the library staff themselves, from an IT consultant in the local authority, to possibly being outsourced to an IT firm completely (Spacey et al., 2015). As well as this, Cooke (2006) notes, not only does filtering represent a different sort of selection process, one that is not necessarily in the librarian's hands and with no clearly defined selection policy, it also relates to the role of the public library – that is, one that educated and informs – and thus the library energy and resources would be better spent educating users. Kranich also stresses the importance of education: "Both children and adults need to be able to assess as well as access information-to distinguish between that which is useful and that which is not. We do not help when we simply wall them off from information and ideas that are controversial or disturbing" (Auld and Kranich, 2005: 199). On the same note, the National Research Council (US) draws a distinctive analogy between accessing content and the swimming pool. A swimming pool can threaten the safety of a child, but that does not mean children should simply be barred from accessing swimming pools:

"A child who knows how to swim is less likely to be harmed than one who does not. Furthermore, teaching a child to swim and to exercise good judgment about bodies of water to avoid has applicability and relevance far beyond swimming pools—as any parent who takes a child to the beach can testify" (National Research Council, 2002: 224).

Educating users about the potential rewards and pitfalls of using the Internet may be a better approach than simply blocking them completely. Teaching children and young adults how to navigate the Internet safely can help to prevent them from accessing potentially distressing material, something that may be prevented if filters are in use (Willard, 2012). This is particularly important with regards to children, who may benefit the most from the opportunity to develop skills in critical thinking about what they access over the Internet, which may be prevented if websites are blocked wholesale (May, 2014).

Another related concern is the loss of agency for the library patron. When perusing the shelves, a patron can choose whether or not to pick up a book. If a website is blocked, they are unable to choose whether or not they want to view it: “if breaking a certain law becomes impossible because of technology, then can humans still exercise individual autonomy with respect to a particular act?” (Tavani, 2007: 43). Being able to access information and express oneself is crucial for autonomy and selfhood (Fried, 1992; Barendt, 2007). As well as producing negative emotions due to feeling controlled, filtering can also simply make the user simply more determined to find the information that has been blocked (Jamali, 2017).

2.2.2 The acceptable use policy

In 1995 Kenneth Lindup noted that in a decade the information security policy had grown from being used by only a select few, to becoming the cornerstone on which computer security rests upon: “information security policies were more or less unheard of outside the world of secret military and government IT networks. Now they are regarded by security professionals as one of the most important of the foundations of information security” (Lindup, 1995: 691). The AUP (also known as computer usage policy, Internet usage policy, or information security policy) is now a vital aspect of facilitating Internet access in corporations (Stewart, 2000; Safa et al., 2016) and is a key document for employees of professional organisations, to maintain awareness of the importance of behaving responsibly with company information on computers and the Internet. Outside of corporate organisations, the AUP has steadily become a key aspect of managing Internet access in schools, universities, and public libraries. Initially, being seen as a way to appease parental concerns regarding the dangers of the Internet (Palgi, 1996), a survey of K-12 schools in the US by Flowers and Rakes found that 82 of the 100 samples had an AUP, with 13 having an AUP in development (Flowers and Rakes, 2000). In public libraries it seems that AUPs have become "almost universally adopted" (Spacey et al., 2015: 73). Willson and Oulton surveyed public libraries in the UK in 1999, with 70% of the 111 respondents stating that a policy for electronic materials was in place, or being developed (Willson and Oulton, 2000). A survey of higher and further education and special libraries conducted in 2003 found that 84% of

respondents had an AUP (Sturges et al., 2003). A survey by Brophy (2003) found that almost all of the 86 responding PLAs had an AUP in place. More recently, a survey of university libraries sent to various electronic discussion lists found that 52% had a web policy (Hendricks, 2006). The FRILLS (Forensic Readiness for Local Libraries in Scotland) project used online surveys to question staff in public libraries, with all respondents stating that they did have an AUP (Poulter et al., 2009). The MAIPLE project utilised online surveys to review managing Internet access in the UK, with 98.8% of respondents stating that they had an AUP (Spacey et al., 2015). Gallagher and McMenemy's analysis of AUPs in Scotland found that all 32 of the public library services had an AUP in place (Gallagher et al., 2015). In general, there is a lack of research on the public library AUP, particularly its content (McMenemy, 2014).

2.2.2.1 What it should contain

In a hierarchical analysis of AUPs, Laughton notes that an AUP cannot be so broad as to contain every single thing, and that it must be concise to be effective.

Laughton states that AUPs are created with three main goals:

- 1. Educating users about activities that may be harmful to the organisation
- 2. Providing legal notice of unacceptable behaviour and the penalties for such behaviour
- 3. Protecting an organization from liabilities it may incur from misuse of the Internet and other computer facilities (Laughton, 2008: 3).

Kelehear states that the AUP should encompass:

- Statement on the intended use and an outline on the advantages of the Internet
- List of responsibilities for users
- Code of conduct administering the use of the Internet
- Description of what constitutes acceptable and unacceptable use of the Internet

- Disclaimer absolving the organisation from possible responsibility of any misuse of the Internet (Kelehear, 2005: 33).

Scott and Voss (1994) note that usage policies should essentially define who can use the service and what they may use the service for. They define a model consisting of seven principles:

- 1. Participation. The policy should involve a committee composed of all user groups
- 2. Partitioning. The policy should be split into a number of sections, each dealing with a separate area of concern
- 3. Philosophy. The underlying principles of the service
- 4. Privacy. How much privacy should users expect
- 5. Persnickety. A list of acceptable and unacceptable usage
- 6. Phog Phactor. The policy should be easily comprehended and any legal or technical aspects explained in an easy-to-understand way
- 7. Publication. The way in which users are made aware of the policy

Describing what should be contained in organisational AUPs, Lichtenstein and Swatman note the importance of a holistic approach. Holistic approaches look at the parts of a given thing as being linked, and explained by, the whole. Lichtenstein and Swatman identified various issues in this approach: legal; managerial; administrative and operational; technical; and human. Human issues were noted as being particularly important, such as recognising employee rights and responsibilities (Lichtenstein and Swatman, 1997).

Doherty et al. (2011) analysed AUPs of 70 academic institutions across the globe. They found that AUPs had eight distinct policy areas: access management; acceptable behaviour; unacceptable behaviour; licence compliance; roles and responsibilities; user monitoring; sanctions for policy violations; and policy management. Similarly, for school library AUPs, Palgi defines four main parts: definition and purpose; rights responsibilities and risks; penalties; and parental consent (Palgi, 1996).

Summarising what was seen to be best practice in the construction of the policy, Sturges suggests that AUPs should have seven essential features:

- Aims and Objectives. It is essential that the policy states the purpose of the service, as this will give context to the other parts of the AUP.
- Eligibility. Who can use the service, including registration details and child access.
- Scope. Service boundaries defining limitations including personal uses, e-mail use, and filtering.
- Illegal Use. Sturges suggests that simply stating “no illegal use” is not helpful without giving some context. This may include references to laws covering data protection.
- Unacceptable Use. This may include accessing material that is legal, but could be offensive to others, or behaviours that may not be acceptable in a public environment.
- Service Commitments. The levels of service provided, including possible disclaimers regarding the service not being responsible for accuracy of the content online.
- User Commitments. What the library requires of the user, including what would happen in the result of a violation of the policy. (Sturges, 2002: 122-123).

Whilst there is some guidance on writing AUPs for public libraries, in the UK each one is written at the local authority level (McMenemy, 2014). Sturges states that an AUP should, at a basic level, define staff procedures and what the service seeks to achieve (Sturges, 2002). The AUP should state the “purpose of the information provision” (Pautz, 2013: 315). Alongside this, the AUP should define what constitutes acceptable use in the public library (McMenemy, 2009), as well as what constitutes as illegal and unacceptable use (McMenemy and Burton, 2005). Sturges notes that as well as defining the procedures for booking terminals and how to deal with technical problems, there should also be information in place regarding “ways to deal with users who do not respect these arrangements” (Sturges, 2002: 105) and “how unacceptable usage is defined and dealt with” (Sturges, 2002: 104). The American Library Association (ALA) recommends all libraries adopt a policy, and as well as

reflecting the library's mission and being updated regularly, the AUP should emphasise freedom of access, as well as setting reasonable conditions for usage allowance and behaviour (ALA, 2007b; 2012). The AUP also expresses what the institution views as the ethical use of computing facilities (Laughton, 2008). As an important legal document, it should also be made sure that it is publicised to library users (McMenemy, 2014). Höne and Eloff state that security policy documents should be created in-house rather than copied from documents by other companies or by searching for Internet samples; doing so could create a "mismatched document that users cannot relate to" (Höne and Eloff, 2002b: 14). By creating something in-house, the security policy document can directly relate to those who will be using it, and can be written in such a way for them to easily grasp. The MAIPLE project included questions regarding the creation of the AUP, which usually involved senior management, legal, library and IT staff, and sometimes councillor contributions (Spacey et al., 2015: 74).

2.2.2.2 Importance of the acceptable use policy

In the public library, the patron must first read and sign the AUP in order to gain access to the library computers and the Internet (McMenemy and Burton, 2005; Pautz, 2013). The AUPs are important for public libraries for a number of reasons: "Policy formulation and documentation is particularly crucial for public internet access service, because it is such a difficult and contentious area" (Sturges, 2002: 104). By transferring responsibility to the user, the AUP provides the library with protection, which can be especially helpful in regards to technology such as filtering; when blocking software is not infallible the AUP can offer good back-up protection (Scales, 2009). As well as protecting the library, the AUP is an important part of making sure that public access is safe (Huang, 2007). An AUP also helps to boost staff assurance when dealing with potential misuse (Heok and Luyt, 2010). Despite its importance for the public library, it is a document which has received relatively little attention (McMenemy 2014).

2.2.2.3 As an educational document

The British Educational Communications and Technology Agency (BECTA) state that an ideal AUP can "help to establish, and reinforce, safe and responsible online behaviours" (BECTA, 2009: 6). A well-constructed AUP is important for giving patrons confidence when using library facilities (McMenemy, 2014). The AUP can act as a guide to safe computer usage, and provide educational instruction regarding library ethics such as privacy. This is particularly important for young people: a number of attitudinal and behavioural intention studies regarding information ethics based on PAPA issues (privacy, accuracy, property, and accessibility) have found privacy has a lower impact on school students than other ethical factors (Masrom et al., 2013; Harncharnchai and Inplao, 2015) with education for young people regarding ethical issues surrounding ICT usage being a key recommendation (Harncharnchai and Inplao, 2015). The AUP can give educational guidance on how to best use the Internet, which can mean providing a way to be less restrictive when providing access: because the AUP facilitates the user in making informed choices over what content to access, it can help negate the need for a filter and possible content restriction (Palgi, 1996).

2.2.2.4 For protection

The AUP is also important for staff as well as patrons. When surveying library staff Poulter et al. notes that library staff "found checking for misuse, and dealing with it, extremely unpleasant" (Poulter et al., 2009). Having a strong, well-written, AUP supports the service and can help to give staff confidence when speaking to users and dealing with possible misuse of the facilities (Rusk, 2001; Heok and Luyt, 2010; McMenemy 2014). The AUP also provides useful protection for the library if the library is wary over the use of blocking software (Palgi, 1996; Kranich, 2004).

The AUP is also a vital aspect of protecting the service from threats: "Even having a basic security policy combined with the right set of tools and technologies can substantially reduce the risk of a serious security incident occurring on your watch" (Sholtz, 2001). Research by Foltz et al. on university policies suggests the presence of Internet policies leads to better

awareness: “Students that received a single exposure to the university computer usage policy reported a noticeably higher level of awareness of both computer usage policies and the consequences of misuse”(Foltz et al., 2005: 144). This has been echoed by Chen et al. whose survey analysis has suggested a higher awareness of the policy results in less Internet abuse (Chen et al., 2008). As well as protecting for potential threats, another important reason for having an AUP is protection against misuse after the fact, and all the legal problems that could ensue (Laughton, 2008).

2.2.2.5 Badly written and ignored policies

Despite its importance, AUPs are often inadequate (Stewart, 2000). Höne and Eloff note that in professional organisations information security policies are seen by users as superfluous and pointless documents that are a waste of time and energy to read: “Quite often, users are ignorant of the policy’s existence; users do not fully understand the document; it is too long or too technical; users do not see the relationship between the policy and their daily tasks and see it as a nuisance” (Höne and Eloff, 2002b: 14). This is exacerbated by policies that are not composed properly or regularly updated, as Laughton states: “Many organizations have not carefully considered the importance of an AUP. It is important that facilities provided are used with good intent, but the importance of computer facilities usage is often overlooked, leading to inappropriate and outdated AUPs” (Laughton, 2008: 3). In their analysis of AUPs from academic institutions, Doherty et al. (2011) found the documents to be highly variable with infrequent updating. AUPs must be written well and kept updated, otherwise there is not much point writing one in the first place, as Scott and Voss state: “If users do not actually read and understand the CUP [Computer Use Policy], the whole effort is wasted!” (Scott and Voss, 1994: 67). An AUP must be a clear and concise document and one that is adapted for the user: “In short, an effective information security policy is an understandable, meaningful, practical and inviting document that addresses the users directly and convinces them of the need for handling information resources securely” (Höne and Eloff, 2002b: 14). It is important, especially for the public library, to get their AUP right and make sure it is seen: “I would suggest that any organisation not only has a responsibility

to develop a good policy, but it also has a responsibility to document it well and make sure that the documentation is capable of reaching the appropriate people. This means that the most up-to-date and authoritative version should be made available from a well-publicised single source" (Sturges, 2002: 103-104).

Höne and Eloff note that a lot of the time, the process of creating the document is left to the technical staff in an organisation who, despite necessarily having lots of relevant ICT expertise, may not be consciously aware that the language of such a document has to cater to those not experienced with technological terminology; if a user cannot understand the language used in the AUP, they can make no real connection to the document, and thus they cannot be expected to know what is acceptable and unacceptable behaviour (Höne and Eloff, 2002a). The policy should be easily read and relatively short (Höne and Eloff 2002b; Pautz, 2013). Palgi states that policies should "avoid excessive use of negative wording" and be "clear and concise. A one-or-two pages policy is better than a longer document full of legalese" (Palgi 1996: 33). This is echoed by Stewart who notes that users will take no notice of a policy full of jargon (Stewart, 2000), and the ALA that states: "Keep it simple and avoid jargon. Making the policy too technical will confuse people" (ALA, 2012: 19). Scott and Voss also emphasise the importance to keep policies concise and readable as part of the Phog Factor in their 7Ps method of writing an AUP (Scott and Voss, 1994). However, it is also important to keep the policy fit for purpose: a survey of various policies from educational institutions, ISPs and non-ISPs, by Siau et al. found that most were worded informally, and were not legally sound (Siau et al., 2002). When surveying public library staff the FRILLS project found that some respondents considered the language of the AUP to be too difficult (Poulter et al., 2009). Laughton states that policies tend to be divided into broad and detailed: "Broad policies are easier to digest but leave grey areas, causing debate. Detailed policies ensure that there are no questionable clauses. Policies should find a balance between being too vague and too technical" (Laughton, 2008: 3).

2.2.2.6 The human element

Even if has been written well, it is imperative that the AUP is actually read. The Open Gateway or Guarded Fortress project used unobtrusive testing to study Internet access in public libraries in the UK, gleaning information on both AUPs and filtering measures. A researcher attempted to visit 14 libraries across the UK and use the Internet within. Of the 12 libraries where they gained access, in two of the libraries staff members helped the researcher log on by going past the AUP screen without a mention, and only one library had its staff member actually explain the AUP and its purpose (McMenemy, 2008; Poulter et al., 2009). When investigating the use of information security policies in healthcare organisations, Gaunt noted that to implement an information security policy asking the staff is a key aspect of ensuring its effectiveness as an informative document: “It became evident that, to be successful, a security policy would need to focus on human factors” (Gaunt, 1998: 132). Höne and Eloff also state the importance of the human element: “At the end of the day, the users will determine how effective the information security policy really is. This means that the information security policy, and all supporting activities, should be completely user focussed — from the writing style and the way in which it is presented to the deployment of the document” (Höne and Eloff, 2002b: 14). This can also extend to the public library AUP; if the library AUP is seen more as a communal document, by both staff and patrons, users may be more invested in it.

2.2.2.7 Being prescriptive

Although the AUP should protect the library and its users from misuse of the facilities, it should also be an educational and informative document for users. Such a document should not rely on being overly focussed on potential misuse, as Rusk states:

“Policies are vital to giving good information services but we must be cautious, as too many policies can erode the creativity and imaginative power of the Internet. When devising “Acceptable Use Policies” to define computer enabled library services it is probably better to understate the “don’ts” and allow for the inevitable patron who is going to use the Internet in the library for some non-research purpose” (Rusk, 2001: 90).

Indeed, Rusk notes that a perusal of policies online tends to highlights what is unacceptable, with threats of possible denial of future access (Rusk, 2001). Likewise, in their analysis of AUPs from academic institutions, Doherty et al. found that in a lot of the AUPs there was an over-emphasis on unacceptable usage and its consequences: “the emphasis is on what users must not do, rather than on what they can and should do, it can be inferred that the AUP has been designed to protect the host institution, rather than proactively educating the user” (Doherty et al., 2011: 208). Ruighaver et al., note that many AUPs are based on deterrence and deontological ethics – i.e. something is intrinsically bad or good – and that this is not effective: “We believe that employees are, in general, no longer accepting the organisation’s word on what is good or bad behaviour, but may be willing to consider the consequences of their actions for the security of the organisation” (Ruighaver et al, 2010: 734). Trialling the use of a more consequentialist-based AUP, Ruighaver et al. found that employees tended to be more on board with an AUP that outlined the consequences of behaviours that did not follow the guidelines. Ruighaver et al. note that AUPs should be formed in a way that is not overtly prescriptive, with good reasons to back conditions that have an ethical foundation: the user will not care if the policy blandly lists do’s and don’ts (Ruighaver et al., 2010). Likewise, Stewart notes that: “it is important to keep in mind that the ultimate objective of the IAUP [Internet Acceptable Use Policy] effort is not so much to catch people doing something wrong as it is to proactively prevent abuse through a well-crafted and well-communicated policy” (Stewart, 2000: 5). Through their discourse analysis of AUPs in Scotland’s public library services, Gallagher et al. found prescriptive or harsh language being used to exert power or discipline over the library patrons, reminding the users that they “are involved in a power relationship” (Gallagher et al., 2015: 582). It is questionable if a patron will feel wholly comfortable browsing the Internet after reading such an AUP, compared to some of the other AUPs analysed, which highlighted the communal nature of the library (Gallagher et al., 2015). Likewise, Moorefield-Lang (2015), notes the heavy focus on rules by library AUPs.

2.2.3 Surveillance

Surveillance in the library includes both physical and electronic monitoring, such as staff members observing users, or screen shadowing software (Poulter et al., 2009). Willson and Oulton's survey of public libraries found that 71% used some form of control on Internet access. This included control software, and also physical monitoring by staff (Willson and Oulton, 2000). The MAIPLE project found that observation by both staff and monitoring software were popular methods of access management, with 83.5% using visual monitoring by staff to help manage access, and 30.4% using monitoring software (Spacey et al., 2015). Similarly, analysis of Scottish public library AUPs by Gallagher et al. found that 91% mentioned that physical or electronic monitoring was in place (Gallagher et al., 2015). Physical monitoring by staff can be combined with computers being placed in public areas to facilitate observation (Willson and Oulton, 2000). Public libraries also use surveillance cameras for monitoring (Newell and Randall, 2013; Randall and Newell, 2014).

Traditionally, the library is seen as a space where free information access is encouraged, and privacy for the patron is of the utmost importance, something that may seem at odds with the use of surveillance. However, surveillance is seen as a necessary tool for protection and as a detector of crime; a "necessary evil" (Barnard-Wills and Wells, 2012: 230). In Denmark, the introduction of staff-less libraries used surveillance cameras to prevent any possible troubles such as vandalism, to help develop a feeling of safety for library patrons, however it also led to issues regarding patron privacy (Johannsen 2012; 2014). This was echoed in Randall and Newell's study of video surveillance in public libraries. Video surveillance was installed as a response to crime, to be used as a back-up in case there are altercations with security staff, and also simply as part of new building designs (Randall and Newell, 2014). Some of the libraries noted concerns over privacy, with one staff member stating "I am at war with myself", and one library system removing cameras in all branches due to privacy concerns (Randall and Newell, 2014: 5). However, it was also noted by one library administrator that "what I'm observing from our patrons is that they care less about their privacy than we do"; the safety concerns and the convenience of different surveillance

measures as well as convenient technology applications such as logging borrowing histories outdid any concerns regarding privacy (Randall and Newell, 2014: 5). Another administrator echoed this sentiment: “you have to work in [a library] to understand the reality of what it is to work in the public library… I’m all for privacy, but safety trumps” adding that patrons should not have expectations of privacy in public libraries (Randall and Newell, 2014: 5). The MAIPLE project also found that some staff favour monitoring as a way to reduce misuse and to create a better space for families (Spacey et al., 2014). Patrons have also responded positively to surveillance in other studies. A survey of over 400 users at higher and further education institutions by Sturges et al. regarding attitudes towards the collection of personal data found that 75% accepted monitoring in the library to prevent misuse (Sturges et al., 2003).

2.2.3.1 For protection

Access management such as surveillance and filtering can help to back-up the AUP. A combined strategy of an AUP alongside access management and monitoring can be effective in curbing potential misuse; an AUP on its own, whilst it can be preventive, lacks the impact of having both approaches (Stewart, 2000). Any service that uses filtering or monitoring should highlight this in the AUP (Sturges, 2002; Pautz, 2013). Physical monitoring by staff can also be used instead of filtering (Pors, 2001).

One of the CILIP’s 12 ethical principles is “Concern for the public good in all professional matters, including respect for diversity within society, and the promoting of equal opportunities and human rights” (CILIP, 2012). Libraries must balance privacy issues with issues of public safety. From a utilitarian perspective, it may be in the public’s best interest to sacrifice some privacy in order to keep the community safe. Allowing unimpeded access to the Internet may be in the best interests of information provision, but the monitoring of such access may help to prevent crime. Indeed, Newell and Randall found that surveillance cameras were being installed in some public libraries as a direct response to concerns by the library staff (Newell and Randall, 2013). The ALA states however, that monitoring duties

is not in the librarian's remit, and is the ethical responsibility of the parents (Wyatt, 2006). Whilst that may be the case, the library is seen as a safe place for children to go, and a lot of parents do expect the library to monitor them: "Some parents even consider the library a babysitter" (Wyatt, 2006: 73). Wyatt notes that a lot of parents *do* see the library as parent stand-in, noting *Kathleen R. v City of Livermore* (2001) in which a parent attempted to sue the library, seeing the library's lack of intervention in her son's viewing and subsequent distribution of pornography a dereliction of responsibility (Wyatt, 2006). Wyatt also notes that if parents do expect monitoring in the public library, and this is not seen to be happening, it may persuade them to prevent their children from using the library, in which case funding for the library may drop (Wyatt, 2006).

2.2.3.2 Surveillance and privacy rights

Gorman notes that "Our privacy is invaded daily; the task is to ensure those invasions are controlled and have benign outcomes" (Gorman, 2015: 181). Is monitoring patrons, physically or electronically too much of an invasion? Gorman distinguishes between the "passive accumulation of anonymised personal data" and the "deliberate, active invasion of privacy" stating that "the former has potential for abuse; the latter *is* abuse" (Gorman, 2015: 185). The library amasses a large amount of information about individual reading habits via the electronic borrowing system. As mentioned by Randall and Newell, logging of patron browsing histories is seen as a convenience (Randall and Newell, 2014). This is echoed by Estabrook who argues that by using reader profiles to target specialised recommendations and services, the public library could help keep the patron interested in its services. Estabrook states that in the current era, so much information is given away, patrons will be well-used to having their details being used by companies and institutions, so the public library's current stance on the information it has and does not use is untenable (Estabrook, 1996). This is also echoed by Mannheimer et al. (2016), who states that holding insistently onto outdated views of patron privacy harms the library, noting that library staff should embrace the abundances of information available to them, such as social networking data. The electronic gathering of browser data might seem similar to the borrowing system –

however libraries monitoring communications such as email may not be as innocuous. Noting the “Faustian bargain” that faces library staff with the potential of Web 2.0, Zimmer (2013) states that education is key; the patron should be well informed of any potential tracking that takes place, that it should be opt-in rather than opt-out, and that the storage of information is minimal, and anonymised (Zimmer, 2013: 53).

Wyatt (2006) notes that librarians are uncomfortable monitoring patrons, however a certain amount of monitoring may be required to prevent users accessing illegal content. Wyatt states that the library’s duty to protect patron privacy is dependent upon how much monitoring is done – differentiating between a member of staff “periodically” walking around the PC area, and patrons’ Internet access being monitored by an “electronic trail” that identifies them (Wyatt, 2006: 77). The use of surveillance in a library setting can damage the patron’s sense of privacy and possibly lead to a chilling effect, an argument that has been made against the use of filtering software in public libraries (Kline, 1999). The ALA (2007a) note the use of video surveillance in particular as having potentially detrimental consequences to a library patron’s sense of privacy, considering its revealing nature. Likewise, CILIP (2011) note that the use of CCTV “raises the question of where the balance of security and privacy should lie” (CILIP, 2011: 14). Again, the library staff must balance safety of patrons with privacy rights. In *United States v. American Library Association* in which Internet filtering was found not to violate a person’s First Amendment Rights, it was noted that filtering software is a far less intrusive measure of protecting patrons from accessing pornography, noting that monitoring computer users could turn the librarian into someone “whom many patrons might wish to avoid” (*United States v. American Library Association* (2003)).

2.3 Conclusion

This chapter discussed the various methods of access management employed by libraries. This is a nuanced, complicated, and at times controversial subject. Methods of access management such as filtering and electronic and physical monitoring are seen as both

protective and overbearing measures, providing patrons with a safer experience and a potentially stifling one equally. The AUP document can provide patrons with a supported means of accessing online content, however the way the policy is written can impact on both the individual and the library service itself. The AUP can inform and educate, but it can also confuse and obfuscate if written badly.

Despite the importance of such a document, the contents of the actual AUP in public libraries has been little researched. As part of the MAIPLE project, AUP documents were analysed on a case study basis, from five different library authorities (Spacey et al., 2014). Analysis of AUP content using Foucauldian discourse analysis was undertaken by Gallagher et al. (2015) on AUPs across Scotland, looking at uses of authoritarian language. McMenemy (2014) also used discourse analysis on a pilot study of 20 AUPs, to analyse AUP content, length, and tone. Access management tools such as filtering have been studied using surveys and the Freedom of Information Act (such as Spacey et al., 2014; Payne 2016), however analysing the use of filtering through the AUP document has only been done on a small scale. This study hopes to build on research such as the MAIPLE project (Spacey et al., 2014), Gallagher et al., (2015) and McMenemy (2014) by expanding the analysis of AUP content in public libraries to the whole of the UK. By analysing the actual AUP document itself, how access management tools such as filtering and surveillance are used, and importantly, how they are communicated to patrons, can be better understood.

The next chapter provides the theoretical framework for this research. The Panopticon will be introduced, and the subsequent surveillance research landscape will be described. Consequentialist and deontological ethics will also be discussed, along with their effect on the public library service.

3 Literature review: theoretical framework

3.1 Introduction

This chapter provides an introduction to the panoptic principle, as well as subsequent surveillance research. This chapter provides a description of the Panopticon, and the surveillance involved that led Michel Foucault to expand the panoptic principle, and its influence on surveillance studies, as well as an overview of surveillance studies more generally, such as surveillance as used in the city, shopping centres, and airports. Panopticism and surveillance studies has blossomed into a wide-ranging area of research. There is also an insight into ethics, and the ethical considerations that govern public library access, such as privacy, access to information, and freedom of expression. Different ethical approaches are described, as well as how these potentially affect library practice. Ethical considerations are an important part of the information profession, and are partly informed in the UK by CILIP's *Ethical Principles* document.

3.2 Panopticon

3.2.1 Introduction

The Panopticon is a type of inspection-house, which relies on the complete exposure of its inhabitants to facilitate it. The idea was brought to the public by Jeremy Bentham (1748-1832), the English social reformer and philosopher who is well known for being a proponent of the utilitarianism strand of ethical philosophy. The idea of the Panopticon originated from his brother Samuel Bentham, in the late 18th century (Werrett, 1999). It was Jeremy Bentham however, that popularised it and brought the idea of the all-seeing gaze to life. Bentham's idea was one of efficiency, and productive labour (Markus, 1993). The Panopticon was first designed as a corrective institution. It was comprised of a circular building, lined with solitary cells, with a watch tower situated in the centre. The cells would house one person each, and because of the shape of the building, the guards in the central tower would have a 360-degree view of the cells, whilst they themselves would remain unseen; Bentham envisioned a system of blinds and special apparatus to help obscure those in the tower (Bentham and Bowring, 1843; Foucault, 1991). Prior to Bentham's ideas,

in the 18th century, John Howard, prison reformer, and William Blackburn, architect, saw the need for space and surveillance to help regulate behaviour (Markus, 1993; Semple, 1993; Morris and Rothman, 1995). John Howard and Jeremy Bentham's ideas both stemmed from a motivation to reform the prison (Semple, 1993). Blackburn thought that the design of the prison could help to maximise the role of the inspector as well as change human behaviour: "Above all Blackburn sought to secure classification and separation; he set the main task of prison architecture as the regulation of human sociability" (Morris and Rothman, 1995: 83).

3.2.2 Design

The design of the building is fundamental to the wielding of power within it. The further inside the Panopticon an individual is, the less they are visible, which gives them more power: "The person with the greatest power is at the tip of a tree, reached through corridors, stairs, outer and inner waiting offices and lobbies" (Markus, 1993: 16). The key to power in the Panopticon comes from the concealment of the guards, who are shrouded in darkness and encased in stone, and the exposure of the inhabitants on the outside ring, vulnerable for all to see: "The overlaying of permeability and visibility defines surveillance" (Markus, 1993: 18). It is a crucial part of the building's design which makes this power possible. In their analysis of 14th century villages in the Western Pueblo region, Graves and Keuren note how such design is important for the social order: "Power can be said to exist in and emanate from the built environment, which structures human action irrespective of those who exercise authority" (Graves and Keuren, 2011: 270). Everyone is linked, by virtue of their position in the architecture, to the central tower. By virtue of its design, with each cell being divided, Bentham understood solitary confinement would make cohesion difficult, preventing the occupants from talking to one another, and would also help to discourage them getting into fights (Markus, 1993). The whole design was to make its inhabitants intensely feel the isolation: "he is seen, but he does not see; he is the object of information, never a subject in communication" (Foucault, 1991: 200).

3.2.3 The unwavering gaze

Due to the design of the building, with the guards in the tower being obscured from the prisoners, whilst they themselves having a complete, 360-degree view of the cells, it was propositioned that cellmates would have to maintain a certain standard of good behaviour, as they would be aware at all times of the potential watchful eye of the guards in the tower. Bentham envisioned using space and visibility to create a reformed and far more productive institution. He thought his idea to be revolutionary:

"*Morals reformed—health preserved—industry invigorated—instruction diffused—public burthens lightened—Economy seated, as it were, upon a rock—the gordian knot of the Poor-Laws not cut, but untied—all by a simple idea in Architecture!*—Thus much I ventured to say on laying down the pen—and thus much I should perhaps have said on taking it up, if at that early period I had seen the whole of the way before me. A new mode of obtaining power of mind over mind, in a quantity hitherto without example" (Bentham and Bowring, 1843 emphasis in original).

Bentham theorised that the pretence of an unwavering gaze, whether absolute or intermittent in reality, gives the inhabitants of the Panopticon the impression they are being watched at all times, and thus they must behave accordingly, meaning that the surveillance is "permanent in its effects even if it is discontinuous in its action" (Foucault, 1991: 201). Due to the invisible and unverifiable nature of the surveillance, the prisoners of the Panopticon will feel like they are being watched continuously, even if this is not actually the case. Bentham described it thusly:

"I flatter myself there can now be little doubt of the plan's possessing the fundamental advantages I have been attributing to it: I mean, the *apparent omnipresence* of the inspector (if divines will allow me the expression,) combined with the extreme facility of his *real presence*" (Bentham and Bowring, 1843, emphasis in original).

Bentham saw the advantages as being able to crunch the numbers in the prison system, along with changing the behaviour of its inhabitants: "the more strictly we are watched, the

better we behave" (Bentham and Quinn, 1843/2001: 277). The omnipresent nature of the observation would, Bentham theorised, lead to the inhabitants internalising the gaze of their watchers and changing their behaviour as if they were being watched continuously – effectively becoming their own guards, and thus negating the need for an extensive workforce. Such a building would be both efficient and productive: "the model of the utilitarian world" (Miller and Miller, 1987: 6).

3.3 Panopticons

3.3.1 Prisons

Despite the fervour with which Bentham campaigned for his dream, an actual Panopticon was never fully realised (Markus, 1993; UCL, 2010). Bentham secured money for a Panopticon, and found land on which to build it, however, as time went on, with more money needed and less commitment from the government, the Panopticon never came to fruition (Semple, 1993; Schofield, 2009). Instead of promoting a better prison system and general utility, Bentham saw the government as only pursuing their own motivations (Schofield, 2009). Buildings were designed with the Panopticon in mind, but they never quite matched the specifications for absolute surveillance capacity: "There were plenty of prisons, hospitals and schools built, and it was certainly the case that there was recognition of the need in these institutions for intermittent surveillance, for careful monitoring at crucial times, but total surveillance was a forgotten dream" (Boyne, 2000: 290). The art gallery Tate Britain, in London, is built on the site of Millbank Prison, which Bentham designed along with Sir Robert Smirke. Although now demolished, there are still areas in the building that resemble parts of the prison (Holtham, 2013). On the Italian island of Santo Stefano, a Panopticon-style prison, closely resembling the San Carlo Theatre in Naples, was built in the 18th century (Branco, 2010; UCL, 2010). Markus (1993) notes the designs for the Edinburgh Bridewell prison by Robert Adam, which uses a semi-circular style, reminiscent of the Panopticon design. Other prisons of the 19th century include the Virginia State Penitentiary, and in Pennsylvania the Western Penitentiary adopted a design very close to the Panopticon

(Dobson and Fisher, 2007). And at Philadelphia's Eastern Penitentiary at Cherry Hill, although not every cell may be observed, the design of the prison "expressed a sense of omnipresent, totalizing surveillance that would imply authority of the commonwealth and its proxies—prison officials—to control the actions of inmates" (Andrzejewski, 2008: 15).

3.4 Foucault

3.4.1 Historical overview

Over 100 years after Bentham shared his idea of an all-seeing, hyper-productive prison, the idea of the panoptic method of surveillance was then explored by French post-structuralist philosopher Michel Foucault, in his landmark work *Discipline and Punish*, first published in 1975. In his chapter on panopticism, Foucault begins with a vivid account of the steps taken to stop the spread of infection in a town fighting the plague in the 17th century. A surveillance system was used, whereby guards patrolled the streets, making sure no-one was outdoors, and everyone was required to make their presence clear in their house in the evenings, by appearing at the window for the guards to see. Foucault described it as "the great review of the living and the dead" (Foucault, 1991: 195). Everyone is made to make themselves visible and known to their overseers; it is a surveillance where presence and absence is key. Foucault described this surveillance as one based "on a system of permanent registration: reports from the syndics to the intendants, from the intendants to the magistrates or mayor**"** (Foucault, 1991: 195).

3.4.2 Self-regulation and the state

Foucault goes on to state that this type of surveillance power can be observed in many other aspects of life, and that it works on a kind of binary system: "Generally speaking, all the authorities exercising individual control function according to a double mode; that of binary division and branding (mad/sane; dangerous/harmless; normal/abnormal)" (Foucault, 1991: 195) and that the Panopticon by Bentham is the "architectural figure of this composition" (Foucault, 1991: 196). Foucault notes the Panopticon's architecture is the opposite of the dungeon: "daylight and the overseer's gaze capture the inmate more effectively than

darkness, which afforded after all a sort of protection" (Foucault, 1972: 2). This overbearing state of visibility in the Panopticon building facilitated what Foucault dubbed an "automatic functioning of power" (Foucault, 1991: 201) and the absorption of the role of the observer in the inhabitants of the Panopticon means that they are caught in a "power situation of which they themselves are the bearers" (Foucault, 1991: 203). Due to the unseen watcher, the inhabitants of the Panopticon modify their behaviour. The constant suspicion that hangs over the subjects being watched induces "heightened self-awareness and paranoia" (Henderson et al., 2010: 235). They internalise the watcher's role and they start to self-regulate their own behaviour. Like Bentham before him, Foucault suggested that effectively, prisoners take on the role of the watcher themselves: the prisoner absorbs the watcher's observation and internalises it so that he becomes "the principle of his own subjection" (Foucault, 1991: 202).

Bentham saw the Panopticon as a dream of industry and invention, and one which could provide a bountiful means of production for the contractor (Himmelfarb, 1965; Markus, 1993) as well as an efficient way of reforming the troublemakers of society (describing it as "a mill for grinding rogues honest" (Munday, 1994: 167)). The Panopticon produces the ideal subject: "passive and pliable" (Spears and Lea, 1994: 438). Foucault's views on the Panopticon are significantly different from Bentham's. Bentham thought his invention humane, and an ideal solution to the criminal justice system at the time (Schofield, 2009). Foucault saw the Panopticon as a struggle of power, "a cruel and ingenious cage" and a grotesque type of social engineering, wherein "visibility is a trap" (Foucault, 1991: 200). The prisoner has become stripped of his personhood: "The individual—-in this case the prisoner—-is an object of study, an object observed while the observer is unseen" (Budd, 2006: 74). Those watching over the prisoners are also in some sense, trapped: "It's a machine in which everyone is caught, those who exercise power just as much as those over whom it is exercised" (Foucault, 2002: 99).

Foucault stated that the panoptic model can be observed in many different institutions outside of the prison system, noting the parallels he found between prison architecture and

those of hospitals, particularly in the late 18th century (Foucault, 1972). He took the building and applied it as a metaphor for a disciplinary society: “He viewed it as an instrument for enforcing discipline and punishment and a means of defining power relations in everyday lives” (Dobson and Fisher, 2007: 308). Foucault suggests that the Panopticon reflects the modern state (Schofield, 2009). Indeed, Giddens states that surveillance is one of the fundamental aspects of modern institutions (Giddens, 1990). The ideal Panopticon is post-structuralist in nature in that the control becomes so effective, the actual architecture is no longer needed: “the process of surveilling oneself becomes automatic, and has no traceable source of origin” (Henderson et al., 2010: 236). Foucault stated that the Panopticon reaches its zenith when the actual building itself becomes superfluous: “the perfection of power should tend to render its actual exercise unnecessary” (Foucault, 1991: 196). The power of the Panopticon should be such that the inmates themselves become their own observers and they internalise the gaze of the unseen overseer. The permeating nature of the observation being such that those under scrutiny absorb the gaze and this then assures the “automatic functioning of power” (Foucault, 1991: 201). In modernity, people govern themselves by self-scrutiny (Bevir, 1999).

3.5 Post-Foucault

Since Foucault, the Panopticon metaphor has been used to inform discussion in a variety of different subject areas such as film, childcare, shopping, policing, and the education system: “This kind of surveillance has become part of everyday life, inculcated and reinforced by social institutions such as prisons, hospitals and schools” (Gallagher, 2010: 263). The work of Foucault has influenced the surveillance field and his theories regarding the Panopticon have helped to inform discussion of state surveillance. In the ‘Foucault Revisited’ special of *Surveillance and Society*, editor David Wood noted one of his colleagues asking: “isn’t every edition a Foucault edition?” (Wood, 2003: 234)

3.5.1 The city

Much work has been done on the use of the Panopticon in the city with the surveillance camera in particular being seen as the symbol of the move towards panopticisation (Norris

and Armstrong, 1999). Norris and McCahill's extensive research has shown the ubiquity of the surveillance camera, particularly in London (McCahill and Norris, 2002) and an international trend towards its deployment (Norris et al., 2004). They note that CCTV can be disciplinary in that it "enables capture, censure and normalisation of particular offenders. It is also disciplinary in that it fosters "habituated anticipatory conformity" by a population that believes it is permanently under surveillance" (Norris and McCahill, 2006: 114). Hille Koskela notes the use of surveillance cameras in urban space, which functions much in the same way as the panoptic prison: "to be seen but to never know when or by whom; under control but without physical intervention" (Koskela, 2002: 293). Like the prison, the inhabitants of urban space are watched over by the camera, but they cannot see who watches them: there is "no 'mutual' gaze" (Koskela, 2002: 298). Noting that spatial relations are crucial to the functioning of the Panopticon, Koskela sees the surveillance camera as the panoptic gaze extended via electronic means and notes the inscrutability of the technology that watches over us: "a surveillance camera is an enigmatic object: it has no eyes but it has the 'gaze'" (Koskela, 2002: 260). Such gazes have a power dynamic like those which Foucault has described (Koskela, 2000). The surveillance camera has multiplied in the city, becoming part of the "street furniture" (Groombridge, 2002: 30), and the type of all-seeing, omnipresent gaze that typifies the Panopticon can be seen in the surveillance camera's presence in public and urban space (Fyfe and Bannister, 1996), including areas with a large surveillance presence such as shopping facilities (Ainley, 1998; Reeves, 1998; Doan, 2010) with the city functioning like a large electronic Panopticon (Ainley, 1998; Koskela, 2000). Norris and McCahill note that the although CCTV can be seen as disciplinary, it is not monitored constantly, and individuals are not necessarily aware of it, so the notion of the CCTV as Panopticon needs to be treated with caution (Norris and McCahill, 2006). Foucault himself also noted that, compared to the institutions of the late 18th century, modern surveillance is much more complicated than simply an all-seeing gaze: "the procedures of power that are at work in modern societies are much more numerous, diverse, and rich. It would be wrong to

say that the principle of visibility governs all technologies of power used since the 19th century" (Foucault, 1972: 2).

Von Hirsch notes that when one is walking in society, they might expect to be noticed by others, but the sustained surveillance from a camera, and the "unobservable observer" (Von Hirsch, 2000: 65) is damaging for individual privacy. In dealing with this "unobservable observer" Goold (2002) notes that there should be certain transparencies in regards to CCTV systems. However, this cannot simply be the names and identities of CCTV operators made known. It is important surveillance cameras are regulated and this regulation requires restriction of public access to make them function correctly, so Goold suggests an agency to watch the watchers. This however, as Goold notes, brings CCTV closer to the Panopticon image, noting the parallels between Bentham's hope that prisons would be better regulated by allowing the public to view the prison, and the external body inspecting the CCTV domain. In his conclusion, Goold asks an important question: "If we are forced to accept that we will never be able to make CCTV surveillance sufficiently transparent to ensure that the presence of cameras does not in some way contravene conventions of anonymity, the question then arises as to whether we should allow such surveillance at all" (Goold, 2002: 27).

3.5.2 Electronic advancements

Suggesting that Bentham's original conception may need some adjustment in the wake of new technology, De Saulles and Horner describe a portable Panopticon – one that is handheld:

"The emergence of mobile technologies changes the dynamics from static, central surveillance to untethered, dispersed surveillance. When we are all capable of covertly recording and then broadcasting the activities of others we may feel the pressure to modify our behaviour in case we are being surreptitiously surveilled by a stranger" (De Saulles and Horner, 2011: 209).

Centralised power is dispersed with the usage of mobile phone camera technology and the general society have become the watchers.

Dobson and Fisher (2007) note that most scholars describe the Panopticon as a metaphor, rather than something to be taken literally. In their study of panopticism and technology, they take the Panopticon as literal and define three generations of the Panopticon:

- Panopticon I: a building, used as a way to perfect society
- Panopticon II: television, an Orwellian device used for enforcing tyranny
- Panopticon III: electronic tracking, for safety and security (Dobson and Fisher, 2007: 308).

Each represents an evolution in technology. The first is the building as imagined by Bentham. The second is the notion of Big Brother as imagined by Orwell in his influential depiction of a totalitarian regime in *1984*. The third is the recent development of Location Based Services (LBS) using technology such as Global Positioning System (GPS).

Similarly, Reiman has suggested the amount of data held by various different companies about us that can be cross-referenced has created a sort of “informational Panopticon” (Reiman, 1995: 44). Like the prisoner taking on the role of the inspector in the Panopticon, Reiman notes that when we are observed, we take on the view of both ourselves and our observer: “This double vision makes you act different” (Reiman, 1995: 41). Reiman notes the importance of teaching privacy: “so that respect for it becomes second nature, and violation of it repugnant” (Reiman, 1995: 44). Likewise, Bakir (2015) notes the use of citizen data, such as that by world governments, is panoptic in nature. As we rely more and more on technology, the masses of data that governments hold and then utilise to spy and target indivduals has a “chilling effect on society” (Bakir, 2015: 18).

3.5.3 School

Michael Gallagher explored the use of surveillance and the panoptic effect in the school and the playground (Gallagher, 2008; Gallagher, 2010). Whilst the school did exhibit aspects of

the panoptic principle, Gallagher also found that it was divergent, most notably in that the surveillance was not absolute, with opportunities to dodge the overseer. Audio and visual observation both functioned, and the use of space in particular, was integral to the surveillance within the school (Gallagher, 2010: 264). At the beginning of Gallagher's fieldwork, the school seemed to be "almost disturbingly panoptic" (Gallagher, 2010: 264). For example, Gallagher notes shock when witnessing the teacher being able to silence the children with her mere presence: "I'm astonished at how she can have such influence over them with so subtle an exertion of power" (Gallagher, 2010: 264). Noting Foucault's remarks about the Panopticon being a machine that everyone is trapped in – both those who exercise the power, and those that are under it – Gallagher witnesses aspects of this in the classroom, with teachers suggesting his presence there is to judge children's behaviour, or the suggestion by the children (jokingly) that "perhaps I was a spy" (Gallagher, 2010: 264). Even Gallagher himself becomes entangled in power play – appeals made by pupils to help in disputes – and thus also, part of the panoptic machine (Gallagher, 2010: 265). It became apparent, as Gallagher's research continued, that the ideal panoptic state is not achieved in the school. Surveillance was discontinuous. The children also often forgot that they were being watched and had to be reminded by the teacher. Also, the source of the surveillance – the teacher – was "difficult to conceal" (Gallagher, 2010: 267). Gallagher finds that despite being deployed regularly in the school, the effects of the surveillance only bear partial resemblance to the Panopticon and that the panoptic model represents the idealised state, rather than a functioning one.

Perryman (2009) notes the use of performance in education, when schools are subject to inspections by the Office for Standards in Education OfSTEAD. Perryman notes that OfSTEAD functions much like the central tower of Bentham's Panopticon, and educators react accordingly, creating a panoptic performance: "in performing for inspectors, management and staff become adept in disguising the real problems and issues which face the school" (Perryman, 2009: 629).

3.5.4 Motherhood

Henderson et al. (2010; 2016) discuss the modern pressure on women to be the perfect mother - which they dub “New Momism” – by using Foucauldian theory as a basis. They note that whilst New Momism is perpetuated through institutional outfits such as the media and health professionals, the most powerful source of pressure derives from the interactions with other mothers. Surveying new mothers via an online questionnaire, they found that lateral surveillance was powerful, and new mothers would start to watch over themselves, much as the inhabitant of the Panopticon would. The respondents displayed “quintessential Foucauldian behaviour” (Henderson et al., 2010: 240) in that surveillance would become automatic, and self-administered. Such internalised pressure then becomes detrimental to the mother (Henderson et al., 2016). A similar viewpoint is studied by Blackford, who notes that surveillance occurs between mothers, and also over the children: “Maternal performances in the public park encode systems by which middle-class mothers govern themselves and one another; through this governance, they also enact and perpetuate governance of children” (Blackford, 2004: 244). Likewise, Caputo, observing middle-class mothers in Canada, notes that mothers and children “enact performances that are highly monitored, controlled and measured according to dominant images and ideals” and surveillance is used to inform good practice (Caputo, 2007: 190). Caputo also notes the intensive watch over children within the school: “On a daily basis, children experience surveillance and control on a number of levels” (Caputo, 2007: 189). Couch et al. (2015) note the use of surveillance during motherhood, particularly by healthcare professionals, and the encouragement of self-surveillance, through the use of media campaigns. Surveillance is panoptic through the repeated clinic visits to ensure the mother and baby’s health are optimal and the use of health information through the media encourages this.

3.5.5 Panopticism in the library

Despite the various avenues of discussion with regards to sociological phenomena such as motherhood, the school, and the city, the panoptic metaphor has been largely ignored in public library research, instead being mostly restricted to historical analysis of libraries.

Leone notes that “panoptic gazes existed within prisons as well as in homes, hospitals, insane asylums, churches, schools and libraries, and forts and mines, all of which were designed for surveillance” (Leone, 1995: 259). There has been research into Foucault, the Panopticon and surveillance in Victorian public libraries (Hewitt, 2000; Black 2001; Black, 2005). Black notes the “intrusive "gaze" of the librarian” (Black, 2005: 416) and the image of the Victorian librarian as a “rule-bound, record-obsessed gatekeeper” (Black, 2001: 71). Hewitt (2000) notes the use of bureaucratic procedures such as the guarantor system. This could be seen as a safety net for the library, to help combat against any losses it may suffer from patrons, however Hewitt notes this security system was in turn used as a “lever with which to improve the conduct of borrowers” (Hewitt, 2000: 80) and that libraries such as the Manchester Free Public Library had promoters who wished working class patrons to show that they were in personal contact (“demonstrated bonds of personal contact” (Hewitt, 2000: 80)) with the middle-class. In the public library’s earlier history, bureaucratic surveillance and control were a significant part of the institution, whether it was in the patrons’ interests or not. Black (2001) notes the use of dynamic surveillance in the Victorian public library: observation of individual patrons and groups, and the use of tracking the individual via administrative means. Indeed, Black suggests that the observant nature of the public library is almost inherent; the design of the public library utilises architecture to facilitate overseeing of the patrons. This can be seen through the use of vast spacious areas that are a feature of the modern public library: the library patron can see around them, but can also easily be seen by those around them, such as the library staff.

Black however also notes that these methods of administration and surveillance are not just necessarily for reasons of control: the public libraries in the Victorian era aimed for “social betterment and enlightenment” and the tracking and administration of patron information was from a “genuine desire to assist the self-realization of users” (Black, 2001: 74). Keeping track of both patrons and books is a necessary administrative procedure for the public library and Black notes that whilst there is a panoptic dimension to the public library in the Victorian era,

which still manifests itself in the public library today, the public library is also an institution for promoting self-expression and rational debate: “their [the public library] avowed aims included the furthering of democratic citizenship and the formation of critical public opinion” (Black, 2001: 76).

More recent studies of panopticism in the public library have included Randall and Newell’s study of CCTV in public libraries. They note the easiness with which panopticism is achieved in modern society through the use of CCTV cameras:

“The Panopticon necessitated a rigid architectural design, so as to achieve the goal of watching without being seen to be watching. However, today this panoptic goal can be achieved in almost any building, thanks to the prevalence of surveillance technologies. It is therefore very easy to draw a contrast between Bentham’s designs and many modern public institutions that have adopted video surveillance technologies, such as public libraries” (Randall and Newell, 2014: 509).

A number of the libraries did not explicitly inform patrons cameras were in operation, nor was there consistent policy surrounding its usage, added to this, one library stated that dummy cameras were in use (Randall and Newell, 2014). These measures – unverifiability, unseen observer, usage of both actual and assumed surveillance systems – point towards a surveillance that is panoptic in nature.

Gallagher et al. (2015) studied AUPs across Scotland’s 32 PLAs. Using discourse analysis, the researchers analysed AUPs to examine themes of power, knowledge, and monitoring. Foucauldian panopticism was found to be highly relevant to the libraries. 91% of the AUPs analysed stated that physical or electronic monitoring was in place. The authors noted that the library environment allows for near-constant monitoring of the library patron, and that whilst the AUP informs the patron of such, the patron will not be able confirm at one particular point if they are being watched or not, and thusly they may start to behave as if they are being watched at all times. It was also found that power was exercised in the AUPs

by using disciplinary and authoritative language. This included language with judgemental overtones, as well as language described as “authoritative and condescending” and large parts of some AUPs being dedicated to detailing sanctions for misuse, which the researchers found to go against what is supposed to be a fairly neutral tone (Gallagher et al., 2015: 586-587). AUPs were also found to discourage patrons from privacy expectations, with one AUP explicitly stating that users should not expect privacy when using the IT facilities: “the unambiguous phrasing of this sentence could be construed as a warning or thinly veiled threat to users” (Gallagher et al., 2015: 583). Making sure the user is aware of the lack of privacy they have, as well as the various monitoring systems documented, gives the impression of a panoptic-style facility: the key to the Panopticon is the extreme visibility of the inhabitants, as well as the constant potential of the watchers.

3.6 Surveillance

In their introduction to *The Surveillance Studies Reader*, Hier and Greenberg reflect on the amount of surveillance that one of the editors – a Canadian – had to go through on a recent trip to the US. After all the different methods of surveillance – on the computer, security checks in the airport, bank cards reading identification numbers – they note the “unrelenting supply of suspicion” (Hier and Greenberg, 2007: 5) that served to make the editor feel “less secure than he did when he awakened that morning” (Hier and Greenberg, 2007: 5). Does the protection of the nation supersede the individual’s right to privacy? What is privacy worth? Moore notes that “Privacy is minimal where technology and organisation are minimal” (Moore, 1998: 292). Privacy is also something that people are willing to sacrifice – be it the surveillance camera in the street, or the biometric checks at the airport, or the monitoring of computer usage in the public library – if it means better protection. However, even when the surveillance being used is ostensibly for the protection of those under its gaze, it does not necessarily do any good for the individual in the short-term, despite potential long-term safety gains: “The technologies might be neutral but the results of their use are not. Clearly camera surveillance can be used by the powerful and occasionally the organised powerless” (Groombridge, 2002: 41). What was once maybe a vibrant landscape can become sterile, as

users of the space are made to conform: “Visibility ensures normalization and control” (Koskela, 2002: 260). Creativity can be lost if one is felt to be under observation. The use of the surveillance camera may be there to watch over its subjects, but at what expense for the individual’s privacy and creative freedom? The use of surveillance cameras may threaten the individual’s confidence in self-expression and free behaviours, as well as impacting on their privacy (Solove, 2002; Kumagai and Cherry, 2004; Rajpoot and Jensen, 2015).

3.6.1 Shopping, television, and the Internet

In a traditional physical shop, the only way to be monitored was by whoever was tending the business that day, and even then, if the shop was busy they would be unable to track everywhere you went inside the building and all the items that you looked at. This has changed with the invention of the surveillance camera and points of sale becoming digital. With surveillance cameras, a security guard can monitor the movements of consumers in store. Even with the use of surveillance technology like this, usage of it is limited to how far the camera can see and is regulated. Compare this with the Internet shop. Browsing the Internet and buying goods online has given companies a treasure trail that Internet users leave for advertisers (Sovern, 1999). Unlike paper records, which take up vast amounts of physical space, electronic data can hold thousands of bits of information in a single file. The declining cost in storing electronic data means organisations do not feel the need to delete information that they hold (Gandy, 2007: 147). Lyon notes that: “Surveillance contributes increasingly to the reproduction and reinforcing of social divisions” (Lyon, 2002: 242). Similarly, Ericson states that the computerisation of information has given rise to the categorisation of who is risky and who is safe: “Innocence declines, and everyone is assumed to be “guilty” until the risk communication system reveals otherwise” (Ericson, 1997: 449). Such surveillance is normalised in the media, where attention is focussed on safety concerns, rather than the wholesale monitoring and data-mining of civilians (Wahl-Jorgensen et al., 2017).

Such is the reliance on digital data and communication, to free oneself of such data-mining would require "opting out of 21st century society" (Anderson, 2015: 160). Of particular concern is the use of surveillance techniques on the Internet, by governments, businesses, and other external agencies. Online, the individual is reduced to a file, or a number in an algorithm, with every purchase made or comment posted being used by marketers, undermining the individual's sovereignty over their personal data and the choices they make Andrejevic (2011). Agencies online, such as social networks, can potentially build up user profiles of individuals before they have even registered with the website, through the use of tracking techniques (Chaabane et al., 2012). The use of tracking and spying on individuals and how they browse the Internet can have a stifling effect on their access to information. Penney (2016) investigated the decline in traffic to Wikipedia articles on topics that potentially raise privacy concerns, after the revelations of the PRISM program in the US and surveillance carried out by the NSA. Noting the substantial decline in traffic post-NSA/PRISM revelations, Penney suggests such surveillance creates a chilling effect for users, noting the potentially harmful implications such as citizens being discouraged to access knowledge and thus being less informed (Penney, 2016). Likewise, Stoycheff (2016) found that individuals are less likely to articulate views that are perceived to be in the minority, if they have been primed of possible government surveillance. Those who supported government surveillance programmes were some of the most likely to stifle potentially dissenting views: "expressing opinions when they are in the majority, and suppressing them when they're not" (Stoycheff, 2016: 307).

Andrejevic suggests that in this era of the online industry, which relies a lot on information gathering, the image of Big Brother is being rehabilitated through the use of reality television, and that surveillance is being shown not as a method of social control, but as "democratisation of celebrity" (Andrejevic, 2002: 251). Surveillance in reality television is used as a platform to acclimatise people to the idea of being perpetually monitored: "The historical reality of Big Brother had changed for this post-Cold War generation. The

totalitarian spectre was gone, replaced by the increasingly routine, annoying but necessary intrusions of commerce in the form of the entertainment industry" (Andrejevic, 2002: 252). Andrejevic notes that participants of reality surveillance television shows are aware of what is happening, and that this is not something that bothers them: "they are neither fooled nor particularly troubled by the commodification of their private lives for mass consumption" (Andrejevic, 2002: 252). Andrejevic states that today, we are captivated with voyeurism and fame; "pathologies of a society in which the public sphere has been eclipsed by the private one" (Andrejevic, 2002: 253). Surveillance is being used as a mechanism to exploit consumers. Consumers take on the role of the traditional market researcher. Consumer interaction means more targeted and more efficient labour. Economy relies on individuality through customisation. This customisation comes by surveillance, and thus surveillance becomes equated with creativeness. Consumers are thus passive recipients of mass-produced products (Andrejevic, 2002).

3.6.2 Terrorism and airport security

David Lyon (2006) questions the security responses in the wake of the events that unfolded in the early 2000s; in an attempt to tighten the security in both the US and the UK following the attacks on the World Trade Centre and the London Underground, various security measures were put in place, such as biometric security, body scanners, etc. In particular, airports have become a vast network of surveillance mechanisms. Technology such as biosurveillance, facial recognition software, and the plethora of surveillance cameras that are peppered throughout the airport building have all sprung up and advanced exponentially (Levi and Wall, 2004). The proliferation of biometric security technology has been a cause of concern: "there is a real and present danger that individuals may simply end up being wrongly identified – or not identified when they should be" (Everett, 2009: 6). As it develops the technology will improve in its accuracy, however it has been noted that multi-modal biometrics give better accuracy (Unar et al., 2014), which possibly raises more concerns regarding privacy invasion. The perceived threat of more attacks means a bigger push to installing more surveillance by various governments, in a bid to assuage fears (Bloss, 2007).

Media outlets continue to use the idea of the "other" to help encourage the use of these surveillance activities (Barnard-Wills, 2011). The apparent benefits of the increase in security measures seem to override any questions of privacy intrusion and whether the extent of the privacy risks to passengers really justifies these technologies being implemented in this way. The idea of surveillance is supposed to make people feel safe and more secure, however, as Gray suggests, more surveillance could add to feelings of insecurity: “there is a threshold point in urban surveillance bond which quantitative change – the addition of devices used and areas watched – becomes qualitative change” (Gray, 2003: 314). Gray notes the use of facial recognition technology, which is part of the burgeoning industry of biometrics, as one that has the ability to transform the notion of privacy itself. Just because there are notices, informing the public of the existence of the surveillance cameras, does not necessarily legitimise their existence: “did the sign informing customers that the area is under surveillance justify the intrusion?” (Hier and Greenberg, 2007: 4)

3.6.3 Does surveillance work to reduce crime

The surveillance camera is often put forward as a major weapon against crime (Wainwright, 2003; BBC, 2015). However, there are doubts to how useful it really is; it is inconclusive whether it actually helps with crime, and its implementation uses large amounts of money (Groombridge, 2008; Taylor, 2010). There are also concerns regarding the potential effects on individual privacy: those who oppose it in the US for example, often point to the Fourth Amendment which states that people have the right to not be unreasonably searched (Priks, 2014). The limitations of this are often discussed in reference to electronic surveillance: for example, *Olmstead v. United States* (1928), which ruled that wiretapping did not violate the Fourth Amendment, and *Katz v. United States* (1967), which then overturned this.

CCTV is often oversold by governments (Gill and Spriggs, 2005), lauded as a kind of “Magic bullet” (Ditton and Short, 1999). Surveying CCTV camera usage in different areas of the UK, Gill and Spriggs (2005) found that CCTV worked best when used with other counter-crime measures, and in car parks and other “small, enclosed areas” (Gill and Spriggs, 2005: 117).

CCTV was not seen to be successful overall: it was expensive whilst not producing results (Gill and Spriggs, 2005). It also seemed to be the case that CCTV was used without proper justification: “There was little emphasis on showing why CCTV was the best solution, only that it was an acceptable one” (Gill and Spriggs, 2005: 118). CCTV was still favoured as a way of combatting crime by the public, even though they did not necessarily feel its intended effects: “although the public for the most part did not feel safer, and despite their perceiving CCTV as less effective than they initially thought, they were still predominantly in favour of its use” (Gill and Spriggs, 2005: 117).

Research has shown that surveillance tends to be most effective in isolated areas. Mikael Priks (2014) analysed the effects of surveillance cameras in football stadiums in Sweden. The installation of the cameras was not done in response to actual crimes, rather it was at the behest of the Union of European Football Associations (UEFA). Prior to the introduction of surveillance cameras, Swedish football stadiums “lagged behind the safety norms issued by UEFA” (Priks, 2014: 1162). Responses from other countries also had an effect on the introduction: it was noted by a senior official that “it is likely that experiences from outside Sweden, in particular from England, led to the decision to use surveillance cameras” (Priks, 2014: 1162). Due to variation in timing of installation, Priks could effectively analyse the before and after effects of the introduction of surveillance cameras. It was found that “the introduction of surveillance cameras in the Swedish soccer stadiums had a very large deterrent impact on unruly supporter behaviour” (Priks, 2014: 1174). There are certain parameters which potentially make surveillance cameras in a football stadium successful. Priks notes that CCTV works well in a “well-contained environment where camera signs are visible” (Priks, 2014: 1164) and where the area is “well defined and easy to monitor, with clearly visible signs and possibly where offenders have a high awareness, and where the penalty might be relatively large given the type of crime committed” (Priks, 2014: 1177). However, Priks also notes that given the concerns around individual privacy “the

effectiveness of the cameras should be clearly evaluated" (Priks, 2014: 1177). What works in one area – such as the football stadium – might not be as effective in another.

Other studies into surveillance have echoed the results of Priks. Using the 1994 terrorist attack in Buenos Aires, which destroyed the main Jewish Centre, Di Tella and Schargrodsky examined the effect of police on car thefts after newly distributed police presence in Jewish and Muslim institutions. They found a "large, negative, highly local effect of police presence on car theft" (Di Tella and Schargrodsky, 2004: 130). Visibility of police presence was key: "a posted and visible police guard exerts a large, negative, local effect on auto theft and little or no effect outside a narrow area" (Di Tella and Schargrodsky, 2004: 131).

Similarly, Akihiro Hashimoto also found that police surveillance in an isolated area tends to reduce traffic accidents. After splitting collision types into cause by driver failure and cause by pedestrian failure, Hashimoto examined how different types of police surveillance set-ups affected driver behaviour. Using different surveillance set-ups at an intersection it was found that "The police surveillance at the intersection seems to have two kinds of effects on the driver. One is that it makes the driver behave better and another is that it makes the driver more alert. The former is temporary and the latter is durable" (Hashimoto, 1979: 269) and "police surveillance at the previous intersection has the effect of making the driver more alert, and it is durable at least at the next intersection" (Hashimoto, 1979: 268). In what appears to be set-up modelled after the Panopticon, Hashimoto found that: "the police surveillance in the centre of the intersection is more effective for almost all collision categories than surveillance from the corner of the intersection" (Hashimoto, 1979: 267). Again, the notion of visibility is key here.

3.6.4 Sousveillance

Fernback (2013) notes the use of "sousveillance", a form of under-surveillance, being used by those protesting large corporations and institutionalised forms of surveillance. The explosion of GoPro cameras have been used in sports, travelling, and to monitor the flying activities of eagles, but they have also been used to monitor crime and police misconduct or

brutality. Even if they are being used for other purposes (such as filming a bike ride for example) these miniscule clip-on cameras can be used to document crimes committed (for example two tourists in Mexico were wearing their GoPro cameras when they were held up at gunpoint whilst cycling (Saul, 2015)) and also to monitor police – particularly during protests and demonstrations (Bland, 2014). Noting that "the digital revolution created an atmosphere in which surveillance is ubiquitous, acute, and naturalized" (Fernback, 2013: 13), and that this can erode our privacy: "Surveillance activities threaten to hurt our freedom and dignity by exposing our private thoughts and private lives embedded in the chunks of data that constitute our behaviours" (Fernback, 2013: 13), Fernback has noted the use of surveillance as a tool to "watch the watchers". Fernback notes that users of social networking sites utilise sousveillance to protest the data-mining habits of companies such as Facebook. One such reaction was against the poorly welcomed Beacon project, which tracked user activity on other websites, and sent the information to Facebook to allow it to target advertisements (Story and Stone, 2007). Protests included a range of activities, such as simply discussing the topic on the social networking website to let Facebook know their awareness of data-mining, and to show resistance, or creating petitions to lobby Facebook into changing its terms or policies (Fernback, 2013). Ultimately this is done in the larger context of mass-scale state surveillance and is a way for citizens to express their contempt for being perpetually monitored and used: "Fundamentally, sousveillance is about exerting control of constant oversight as a potential force for democratization" (Fernback, 2013: 14).

3.6.5 The surveillant assemblage

Rather than a panoptic style scenario in which an all-encompassing overseer surveys the population in a state of control, Haggerty and Ericson (2000) suggest instead that modern surveillance is more a web that we are trapped in: no-one is above it, no-one is outside of it. The notion of the large, circular prison as envisioned by Bentham and then Foucault, whilst still a helpful metaphor, does not adequately cover the insidious and rapidly expanding nature of contemporary surveillance. Surveillance is not limited to certain groups of people, nor is the control of it confined to the upper echelons of the state. Haggerty and Ericson

remark upon the “massive efforts” (Haggerty and Ericson, 2000: 607) of both state and non-state institutions in their monitoring of society, and also the “extension and intensification of surveillance across all sectors of society” (Haggerty and Ericson, 2000: 607). For Haggerty and Ericson, although the metaphor of the Panopticon is a helpful one, it does not take into account the all-encompassing force that surveillance has become. Modern surveillance is likened to the rhizomatic expansion of plants. The botanical rhizome consists of a stem underground that sends out new roots, if separated they can form new plants, making growth potential quite extensive (Rudall, 1984; Colombat, 1991). The idea of rhizomes in a philosophical sense was developed by Deleuze and Guattari in *A Thousand Plateaus*. Instead of a hierarchical, linear concept of knowledge, they describe a non-hierarchical concept of knowledge, with multiple exit and entry points for data (Deleuze and Guattari, 1988). *A Thousand Plateaus* is written in such a way that any of its main points are immediately connectable to other points making it difficult to summarise (Smith and Protevi, 2018). The rapid expansion and conglomeration of various surveillance systems, once discrete and now absorbed, reflects this. Haggerty and Ericson take this concept of overlapping and expansion and apply it to surveillance theory, which they term the surveillant assemblage: “The concept of the surveillant assemblage describes the converging nature of what was once discrete surveillance systems” (Hier, 2003: 399). They also state that modern surveillance breaks down the body into bits of data and then reassembles it into a “data double” (Haggerty and Ericson, 2000: 611) which is then sent back to the individual. And, rather than being a top-down control system, surveillance has moved beyond that state, and is both accepted and even encouraged by those who are under its gaze (Haggerty and Ericson, 2000).

The notion of the surveillant assemblage, however, does not necessarily account for the targeted scrutiny that has become routine in spaces such as airports. Hier notes the burgeoning use of biometric surveillance and surveillance camera monitoring used in such areas and states that “although surveillance may be rhizomatic today, the shoots that the

assemblage spawns are always amendable to incorporation by a range of political agendas and aspirations and often enjoy popular support ”(Hier, 2003: 410). Modern surveillance may be indeed, a rhizomatic assemblage in which everyone has been ensnared, however, at the point of deployment, behind the surveillance camera or the use of biometric data technology, there is someone who has authorised the use of such mechanisms. Taking the idea of Thomas Mathiesen’s concept of synoptic (bottom-up) surveillance, where the many watch the few (Mathiesen, 1997), Hier collects these different notions of surveillance and suggests that: “scholarly discourse may better appreciate the social and cultural foundations to the selectivity of the surveillant gaze as the culmination of synoptically mediated desires towards the panoptical aspirations of order and social control” (Hier, 2003: 410). As Hier notes, this rhizomatic expansion is not by chance, nor is it motivated by unconscious thought. This overlapping of surveillance systems (called “leaky containers” by Lyon (2001)), such as the convergence of public and private data storage systems (Hier and Greenberg, 2007) help to form new “surveillance dimensions” (Marx, 2007: 84), with new technologies allowing surveillance to be so natural as to be almost unnoticeable as it becomes “integrated into routine activity” (Marx, 2007: 88). This then helps to both boost the scope of discrete systems, and also makes the sharing of information effortless. Marx (2006) notes the difference between hard surveillance – that is, surveillance by coercion or threat – and soft surveillance – surveillance by a more seductive means, or gentle coercion, such as that of consent, sometimes by implication rather than explicit direction. This idea does help with Haggerty and Ericson’s idea of visualisation, but it is certainly still a method of control.

3.6.6 Care and control

Surveillance is part and parcel of modern life (Haggerty and Ericson, 2000; Groombridge, 2002; Lyon, 2002; Monahan, 2011). Surveillance, especially automated surveillance, has become an integral part of daily life in society: "Surveillance is "designed in" to the flows of everyday life" (Rose, 1999: 234). Surfing the Internet, going to the bank, voting in an election, and paying various bills utilises various aspects of surveillance, observation, and the verification of identity. Simply walking down the street in a big city involves individuals’

faces being caught hundreds of times on various surveillance camera systems. At school, surveillance cameras are being deployed to combat misbehaviour and crime (Harris, 2011; Paton, 2014). Surveillance is also used by the state for welfare reasons: protection via surveillance cameras, distribution of state benefits, healthcare treatment efficiency, to name but a few. However, the recording and tracking of information that has become so routine in our everyday lives also places individuals into categories, which helps to encourage social division (Lyon, 2002: 245). A lot of surveillance is used to categorise us; the customer loyalty card takes our shopping habits and our demographic information and assigns us to a designated customer type that is used to target for goods and services. The biometric data reader at the airport assigns us to a certain category dependent on our level of threat. Bureaucratic administrations use surveillance to be more efficient, but also to categorise us: the monitoring of who is receiving welfare, and if they are trying to "play" the system. Indeed, the categorising nature of surveillance is integral to it: "social sorting characterizes just about all contemporary surveillance systems" (Monahan, 2011: 498).

However, even when there is suspicion that surveillance may be being used for controlling or conforming purposes, the effects can be questioned when examining the reactions of those under scrutiny – the surveillance objects. Zurawski, for example notes that even when consumers are aware they are giving away their personal data in exchange for a customer loyalty card, they are not bothered by this. In fact, this may just be subsumed into the larger shopping experience, and becomes part of the shopping narrative (Zurawski, 2011). The loyalty card is part and parcel of the shopping experience: "a cultural practice in its own right" (Zurawski, 2011: 511). However, even when consumers are aware that they give away data in exchange for their customer loyalty card, how many of them are aware just how much and to what extent the data they provide is being mined for demographic information for company profit? On one hand, the loyalty card is an object, used for gain by the customer, and on the other it is the gateway for the corporation to gain access to valuable shopping habits and information provided by the customer (Lyon, 2003). It is often done so effortlessly

that the consumer may barely even notice it is happening: “We gladly, if often barely consciously, give up this information in return for the ease of buying and communicating and the seductions of frequent flyer and other reward programs” (Marx, 2006: 2). Ariane Ellerbrok (2011) takes the example of commercial automated facial recognition system applications. These systems, used for example by users of Facebook, can link names and faces. Whilst it is promoted as being both fun and entertaining, a type of social game, there is a darker side concerning marketing programs as fun and frivolous that are then used to mine user data for large corporations. However, as Monahan notes, whilst this line of enquiry should be investigated, the agency of those being monitored and mined for information should not be dismissed: “it can be insulting to begin from a position that presumes people are dupes and that they simply do not understand their situations as clearly as do researchers” (Monahan, 2011: 500).

Different aspects of surveillance such as these serve to demonstrate how nuanced the topic of surveillance, and its impact on privacy and freedom, is. Although there are concerns over individual privacy and the potentially nefarious uses of surveillance, much of what surveillance is used for is to help and enhance our daily lives: "Although the word surveillance often has connotations of threat, it involves inherently ambiguous processes that should not be considered in a merely negative light. Much everyday convenience, efficiency and security depends upon surveillance" (Lyon, 2002: 242). Lyon also notes the paradoxes surrounding the supposed threats of surveillance: "Privacy, which so often is felt to be endangered by these developments, can equally be considered as a key generator of surveillance" (Lyon, 2002: 245). The need to protect one's privacy has generated the use of credentials and tokens of trust. One needs documentation to be trusted or accepted by certain groups, and this use of documentation and tracking undermines one's privacy. The same can be said regarding the efficiency of administration in organisations: surveillance is an effective way of maximising efficiency.

Thusly, there are arguments that surveillance is detrimental to privacy, and erodes civil liberties, and arguments that surveillance is helpful for protecting people and preventing crime. David Lyon sought to reconcile the positive and negative aspects of surveillance by way of introducing the care and control continuum. Lyon stated that rather than strictly being one or the other, the use of surveillance lies instead on a continuum: at one end there is the notion of care and the other, the notion of control (Lyon, 2001). The control side taps directly into the panoptic effect: using biometric surveillance, such as facial recognition data, to try and ensure adherence to airport rules, or Internet filtering to make sure computer users can only access certain types of website. The caring side serves to protect and look after citizens, such as surveillance cameras in a rest home for the elderly to ensure proper care is being carried out or GPS tracking on mobile phones in case they become lost or stolen. Some types of surveillance can (and often do) occupy both ends of the continuum (Monahan, 2011). Customer loyalty cards are on the one hand, helpful to the consumer by giving them benefits such as monetary rewards, however they are also controlling as the customer then feels bound to shop in a particular store otherwise they will lose out on rewards, and their data is mined by the company for information on demographics and the shopping habits of its consumers. The care side of surveillance goes to protect and serve, and look after those who are being monitored, whilst the control side serves to impose certain behaviours. Lyon likens surveillance to the Roman god with two faces, Janus (Lyon, 1994; 2001). This new viewpoint serves to demonstrate that nefarious notions do not necessarily highlight the nuances or complexities of surveillance: surveillance "often operates simultaneously in both of these registers (care and control)" (Monahan, 2011: 497).

Another aspect on the nuances of surveillance is Marx's notions of hard and soft surveillance, involving both threatening and gentle coercion. Sometimes this is dressed to look like it is voluntary, even when it is not, such as the notices in buildings stating that those entering agree to be searched: Marx notes the "disingenuous communication that seeks to create the impression that one is volunteering when that isn't the case" (Marx, 2006: 2). As

Monahan (2011) observes, the Foucauldian outlook on surveillance also tends to focus on those who conduct the surveillance, and their aims, rather than that of those who are under the scrutiny of the surveillance. However, as Dobson and Fisher state, control may not be the watcher's intention, but this is easier said than done: "Control may or may not be intended. Rare, however, is the "inspector" who can watch and know and yet resist the temptation to influence the subjects' actions to one degree or another" (Dobson and Fisher, 2007: 312).

The next part of this literature review looks at different approaches to ethics and how this is manifested in the library.

3.7 Ethics

Ethical considerations are an important part of the library profession. This is especially true of access to the Internet and other digital services. Two approaches to ethics deal with the outcome of an act and the intrinsic nature of the act itself. These are consequentialism and deontological (also known as categorical) ethics. Consequentialist moral reasoning is where the morality lies in the consequences of an act, and deontological (or categorical) moral reasoning is where the morality lies in the intrinsic nature of an act. Consequentialism is concerned with the effects of actions, whereas deontological reasoning states that we must take certain paths, regardless of the outcome.

3.7.1 Consequentialism and utilitarianism

The most well-known branch of consequentialist moral reasoning is utilitarianism, made famous by Jeremy Bentham and John Stuart Mill. Utilitarianism states that the best course of action is the one in which the majority of people are happy, or the "utility" is maximised: "More specifically, a policy is the morally correct one if, and only if, it promotes more overall (or net) happiness than any other alternative policy; otherwise, it is wrong and ought to be rejected" (Doyle, 1998: 48). Bentham suggested the concept of utilitarianism could be applied to legislation, as well as individual actions, and he came up with a number of ideas to maximise utility. These included taking beggars off the streets and putting them into

workhouses (Bentham and Bowring, 1843), as well as the aforementioned Panopticon. Utilitarianism is appealing because everyone's wants are placed on the same level: "all preferences count equally" (Sandel, 2010: 52). It is an appealingly simple way of analysing right and wrong: pleasure is good and pain is bad (Hart et al., 1789/1970). It looks to the consequences of actions, and it analyses them in a straightforward way: is utility increased? There are a number of arguments against utilitarianism, the most glaring of which, Sandel states, is the failure to respect individual rights (Sandel, 2010). Utilitarianism, by trying to give the best situation for the most amount of people, tends to place individuals on a scale, and individual rights become subsumed underneath the needs of the majority. This has been illustrated by some interesting thought experiments, such as the runaway tram case: would it be ok to change the direction of a runaway vehicle such as a tram if it kills someone, in order to save five people it would have killed if left on the same course? (Foot, 2002). Or Ursula Le Guin's tale of one city's joy at the expense of a child who lives in misery (Le Guin, 1993). Likewise, views of torturing people for information: utilitarianism possibly allows for torture of an individual if enough lives will be saved with the information gained. John Stuart Mill tried to reconcile individual rights with utilitarian philosophy. Mill suggested that individuals should be allowed to live independently: "Over himself, over his own body and mind, the individual is sovereign" (Mill, 1985: 22). By respecting the individual's rights and free will, with the only caveat being that the individual should not harm others, utility will be gained. By respecting individual liberty, utility will be maximised in the long run: utility is the ultimate appeal, in the largest sense (Mill, 1985). By defending individual rights so stringently however, Mill's stance could be seen as going outside the confines of utilitarianism (Sandel, 2010).

3.7.2 Deontological and Kant

The most famous categorical moral reasoning comes from Immanuel Kant, the 18th century German philosopher, who stated that moral worth comes from the intrinsic nature of an act, and not the results of it: "A good will is good not because of what it performs or effects, not by its aptness for the attainment of some proposed end, but simply by virtue of the volition; that is, it is good in itself" (Kant, 1785/1948). People should choose to do something

because it is inherently right, and not because of any potential end result. Kant also proposed that people should be treated as ends in themselves. Kantian ethics looks for individual motives and looks after individual rights. In *Groundwork of the Metaphysic of Morals* his categorical imperatives state that:

- People should act in such a way as if their actions were a universal law.
- People should be treated with dignity, and not as a means to an end (Kant, 1785/1948).

Kant's philosophy has a special focus on individual rights which clashes with utilitarianism as it treats people as a means to an end (achieving the maximum utility regardless of the means in doing so). Kantian ethics is also quite stringent in its approach; the universal law to which someone subscribes should be just that – universal. If lying is wrong, it must always be wrong, no matter the circumstance or the outcome. People should not be treated as a means to an end, but with dignity, as ends in themselves.

Both consequentialist and deontological ethics can allow for the same outcome. In the case of torture for example, Sandel (2010) notes that utilitarianism may reject torture on the grounds that it does not work and therefore does not raise utility. Whereas deontological reasoning might state torture is never just, and individual rights trump the use of torture even if it were to be successful.

3.8 Access to information and freedom of expression

Access to information and freedom of expression is a fundamental right, enshrined in the *Universal Declaration of Human Rights*. Article 19 of the *Universal Declaration of Human Rights* states that: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". This is also echoed by other conventions such as the European Convention on Human Rights and Fundamental Freedoms, and in statutes such as the First Amendment of the Constitution of the US, and Article 10 of the UK *Human Rights Act*.

From an ethical standpoint, freedom of expression can be seen as fundamental from both deontological and consequentialist ethics. John Stuart Mill and Immanuel Kant, two of the most famous thinkers on consequentialist and deontological ethics both argue for freedom of speech. John Stuart Mill and John Milton both argue for freedom of expression as a way to arrive at truth. In his *Areopagitica*, John Milton states that individuals have reason, and free will, thus they should be allowed to judge for themselves whether an idea is good or bad (Milton, 1644/1973). In *On Liberty*, John Stuart Mill argues that all doctrines should be heard, as a "matter of ethical conviction" and individuals have a duty to form the "truest opinions they can" (Mill, 1859/1985: 39). Mill is a staunch supporter of freedom of expression and claims that everyone's ideas and opinions should be heard, no matter how immoral one may find it: ideas must be critiqued to get to truth. This is also discussed by Thomas Nagel, who notes that by banning material that argues certain concepts (such as the denial of the Holocaust) suggests those concepts are not able to be defended: "that they are so vulnerable to denial that they need to be given the status of dogma, protected against criticism and held as articles of faith" (Nagel, 1995: 98). Ideas should stand up to scrutiny, and this is how one arrives at the truth. If they cannot stand up to scrutiny, perhaps they need to be dispensed with altogether. Mill's only condition of freedom of expression is what has been called the "harm principle", and that is:

"the sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number, is self-protection. That the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others.. His own good, either physical or moral, is not a sufficient warrant" (Mill, 1859/1985: 23).

To obtain real truth, discussion must be "open and unfettered" (Doyle, 1998: 241) and no matter what the opinion, it must be given time to be heard: "All ideas, even the most offensive, preposterous, or potentially injurious to be expressed and canvassed should be allowed; even those opinions that seem so well established as to be beyond controversy"

(Doyle, 1998: 241). Censorship, for Mill, can only obscure and hinder, rather than help: “In sum, censorship of ideas inhibits the emergence of truth, and inhibiting the emergence of truth undermines overall happiness. Any practice or policy that undermines overall happiness ought to be rejected. Therefore, censorship of ideas ought to be rejected” (Doyle, 1998: 241).

As well as the perspective of discovering truth, Barendt defines three other common justifications for freedom of speech: the right to self-development; citizen participation as part of democracy; and suspicion of government (Barendt, 2007: 6-7). The self-development justification argues that individuals should have the right to express, think, and judge for themselves and that this is a fundamental part of being a person (Fried, 1984; Barendt, 2007). The right to self-development argument for free speech stems from the concept of autonomy: Kant’s idea of the right to be treated as an individual and not as a means to an end. Autonomy has been argued as the underpinning of all basic liberties (Fried, 1984) and has been linked with other arguments for rights, such as voting rights, freedom of religion, and bodily rights such as the freedom to use contraception (Brison, 1998). By denying freedom of expression on the grounds of censorship for example, is akin to saying someone has no mind of their own. As Nagel states: “The censorship of a fanatical bigot is an offense to us all” (Nagel, 1995: 98).

The democracy argument for freedom of speech states that having freedom of expression is a cornerstone of a democratic society (Fried, 1984) and that a democratic, self-governing society needs to be well-informed (Meiklejohn, 1961; Schauer, 1982; Alexander and Horton, 1983). One of the most famous views on the democracy argument comes from Justice Brandeis’s concurrence in *Whitney v. California*. Speaking on the principles of the Founding Fathers, Brandeis noted that: “They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth” (*Whitney v. California*, 1927). This argument for freedom of speech is utilitarian in nature: a democratic society is served best and utility will go up if freedom of speech is allowed to

flourish (Barendt, 2007). Post argues that having autonomy is also a vital component for the democratic defence of free speech (Post, 1993). Baker notes that freedom of speech is valuable for a variety of reasons, but autonomy is one of the most important, because democratic society depends on the autonomy of its citizens to function: “The legitimacy of the legal order depends, in part, on it respecting the autonomy that it must attribute to the people whom it asks to obey its laws” (Baker, 2011: 251).

The argument of government suspicion for freedom of speech emphasises the potential malevolence of free speech being stifled. These actions can prevent knowledge and legitimate information from being spread (Schauer, 1982; Barendt, 2007). Authorities may be wary of subversive ideas and use legislation as a way to discredit individuals (Barendt, 2007). This is also connected to the chilling effect, defined by Schauer thusly: “A chilling effect occurs when individuals seeking to engage in activity protected by the first amendment are deterred from so doing by governmental regulation not specifically directed at that protected activity” (Schauer, 1978: 693). Limiting certain parts of freedom of expression could have the knock-on effect of limiting or discouraging others from expressing their own, perfectly legitimate views.

3.8.1 Freedom of expression in the public library

Freedom of expression and access to information, alongside and intertwined with privacy rights are held as fundamental aspects of the public library service. Indeed, most library associations regard privacy and access as top priorities (Juznic et al., 2001). Both the ALA and CILIP regard freedom of expression and access as important ethical principles of the profession:

- “We uphold the principles of intellectual freedom and resist all efforts to censor library resources” (ALA, 2008a).
- Ethical Principle 3: “Commitment to the defence, and the advancement, of access to information, ideas and works of the imagination” (CILIP, 2013).

Freedom of access and expression are important to the librarian because it is one of the main tenets of the profession. Providing access to knowledge and works of the imagination is one of the foundations of the role of the librarian (Gorman, 2015). Ranganathan's first of the *Five Laws of Library Science* states that: "Books are for use" (Ranganathan, 1957). At the fundamental level, this means the library service should support access to information (McMenemy, 2009). Access to information, and access to ICT resources in particular are valuable for communication and democracy (Johansson, 2004; Shirazi et al., 2010). This is particularly important in the public library, which helps those who might not otherwise have access (Sigler et al., 2011; Pautz, 2013).

3.8.2 Limits to freedom of expression

Freedom of speech and the possible limitations put on freedom of speech has become a large and difficult issue (Spinello, 2016). The Internet and its vast capabilities have given individuals a huge arena to express themselves, and considerable controversy has arisen between those wanting to express their thoughts and those wanting to control what is regarded as offensive or hateful views.

For many in the library profession, the advice of D.J. Foskett, in his seminal book *The Creed of a Librarian: No Politics, No Religion, No Morals* is a key touchstone for professional ethical judgement. Foskett suggested that the librarian's attitudes and personal beliefs should not affect the library patron in any way. In fact, the librarian should be so neutral they "ought virtually to vanish as an individual person" (Foskett, 1962: 10). Hauptman however states that steadfastly sticking to the principle of freedom of access, no matter what the situation is akin to having no independent thoughts at all: "If they [information professionals] do not think and make adjustments, they have missed the most important aspect of the pedagogical process. It is all too easy to confuse education with indoctrination, and a cadre of indoctrinated professionals is oxymoronic" (Hauptman, 1976: 627). Being a slave to neutrality could have adverse effects if the librarian is to also be socially responsible and the stance of being absolutely neutral can be easily used as a shield: "Censorship is never

warranted, but it should not be confused with a refusal to aid and abet egregiously anti-social acts in the name of some higher obligation. Claiming that patrons may only be interested in reading about something is an easy way to avoid rendering a difficult judgement" (Hauptman, 1976: 627). While it is true that it is not the same as censorship – refusing someone material or information is not the same as an outright ban on said material – if the public library is the only place of information for someone, then it may feel like they are being subjected to censorship.

With this problem of ethics and freedom of access in mind, Hauptman set out to test the ethics of librarians, both public and academic, by going into 13 libraries and asking the librarians on duty to help him locate information about the substance cordite – a low explosive – and its potency: "whether a small amount will blow up, say, a normal suburban house" (Hauptman, 1976: 626). Every single person he asked had no qualms regarding the morality of the request; indeed, one particular member of staff figured out the crux of why he was asking for such information and was unbending in her approach: "The nature of the request is irrelevant; the librarian does not have the right to discriminate against a patron" (Hauptman, 1976: 627). Hauptman however, disagrees: "To abjure an ethical commitment in favour of anything, is to abjure one's individual responsibility" (Hauptman, 1976: 627). Hauptman states that, rather than being an affirmation of one's professional obligation, to dispense information no matter what the request, and to use freedom of access as a defence is hiding behind a shield and casting off any accountability: "Aiding and abetting a heinous crime in the name of what I have termed a dubious commitment to information dissemination and then claiming that a professional organisation's code calls for this is an abjuration of personal responsibility and a highly unprofessional act" (Hauptman, 1976: 627). A categorical view might be that if freedom of access is sacred in the library, then no matter what the circumstance, the patron should have access to the materials they require. But then is it perhaps better for the majority if patrons wanting materials for nefarious purposes are denied their requests, even if it means also refusing items to patrons who are simply

genuinely interested in the subject matter? Or by protecting every individual's right of access, it may be better for everyone in the long run: by looking after every individual's right to access, the majority are then benefitted from feeling free to access the materials they wish. As acknowledged previously, John Stuart Mill himself was against censorship. In order to be truly happy, Mill theorised that society must seek the truth, and to obtain this truth, all ideas must be heard:

"But the peculiar evil of silencing the expression of an opinion is, that it is robbing the human race; posterity as well as the existing generation; those who dissent from the opinion, still more than those who hold it. If the opinion is right, they are deprived of the opportunity of exchanging error for truth: if wrong, they lose, what is almost as great a benefit, the clearer perception and livelier impression of truth, produced by its collision with error" (Mill, 1859/1985: 52).

The library however, has to take every patron into account, and whilst they should protect someone's right to access material, do they not also have a duty of care towards those who wish to be shielded from disturbing material – especially if it is displayed on a screen that they can easily see? (Young, 1997).

Since Hauptman's famous bomb experiment, others have tested how willing librarians are to disseminate information with similar results. Robert C. Dowd asked various librarians about drug use such as how to freebase cocaine. As with Hauptman, no-one refused him help. Unlike Hauptman, Dowd found this to be a positive result and a commitment to freedom of access noting that: "anyone should have the right to read about either explosives or cocaine" (Dowd, 1990: 493). Similarly, Juznic et al. (2001), like Hauptman and Dowd, approached librarians to find out whether ethical principles would prohibit them from dispensing information. The researchers approached 52 librarians in all, to ask about information on various sensitive topics, including suicide and necrophilia. Much like the other studies, they found the librarians' willingness to help them was unaffected by personal attitudes towards the topics at hand (Juznic et al., 2001). Noting the Slovenian library code of ethics they state

that “Librarians must give information assistance which is requested, even if the possible use of the information by the patron may be personally objectionable to the librarian” (Juznic et al., 2001: 76). In fact, the more pertinent points were limitations in knowledge and lack of expertise (Juznic et al., 2001). Dowd and Juznic et al. invoke Kant’s categorical moral reasoning here, suggesting that a commitment to the individual, and that privacy and freedom of access should be absolute, rather than dependent on circumstance. Hauptman appeals to the utilitarian stance; it is better to think about how each decision will affect the whole community. G.A. Marco states that while there should be a balance, ultimately the librarian should be utilitarian and serve the community, and thus the greater good:

“How we decide to treat a patron’s reading or reference records is determined by our competence to judge the risk to that greater good (’Clear and present danger’ is a useful guide). There is no duty/desire decision, but a duty/duty decision, in which the higher duty to community takes automatic precedence over the lesser duty to the individual patron” (Marco, 1996: 35).

3.9 Privacy

Privacy is defined by the *Oxford English Dictionary* as: “A state in which one is not observed or disturbed by other people; The state of being free from public attention”. In 1890, Warren and Brandeis wrote about controlling one’s personal information and personality, noting the recent developments in newspaper coverage encroaching on people’s personal lives. They noted that individuals should have the “right to be let alone” and they regarded protection of individual privacy as important for society: “the protection of society must come mainly through a recognition of the rights of the individual” (Warren and Brandeis, 1890: 219-220).

A lot of descriptions of privacy rights define privacy in relation to controlling information about oneself. Fried (1984) states that controlling access to yourself is essential to privacy. Westin states privacy is: “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1967: 7). Whereas Reiman (1995) states that rather than controlling the access, it is

depriving others of access that is the right to privacy, and by being able to do this, gives the individual self-ownership. Gavison states that privacy is related to accessibility to oneself: "the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention. This concept of privacy as a concern for limited accessibility enables us to identify when losses of privacy occur" (Gavison, 1980: 423).

Like arguments for freedom of expression, privacy is also argued as being essential for autonomy and a person's self-development. Moore states that being able to control access to ourselves and our personal information is an "essential part of human flourishing or well-being" (Moore, 2003: 223). Cohen also states that privacy is essential for the self – giving individuals autonomy – and a lack of privacy means less potential for self-development: "It enables situated subjects to navigate within preexisting cultural and social matrices, creating spaces for the play and the work of self-making" (Cohen, 2013: 1911). In a similar vein, Bloustein (1964) notes that privacy is essential for human dignity. Discussing Warren and Brandeis's influential paper on the subject, Bloustein states that having a person's personal life be fodder for the press would "destroy individual dignity and integrity and emasculate individual freedom and independence" (Bloustein, 1964: 1971).

3.9.1 Privacy in the public library

Privacy is one of the fundamental principles featured in library ethics codes and the privacy of users is an important and essential part of the profession (Sturges et al., 2001; Woodward, 2007). An international review of eight library ethics codes by McMenemy et al. found that patron privacy was a concern raised by almost all codes reviewed (McMenemy, et al., 2014). The ALA states that "privacy is essential to the exercise of free speech, free thought, and free association" (ALA, 2008b). Privacy is enshrined as part of CILIP's *Ethical Principles* document, summarised as: "Respect for confidentiality and privacy in dealing with information users" (CILIP, 2013). Gorman notes that privacy is important for practical and moral reasons in the public library: library users need to be able to have trust in their librarian

with their information, and exercising rights like freedom of expression and access will not work without privacy (Gorman, 2015). Despite this, in a 2003 survey of libraries in the higher and further education, and special library sectors, Sturges et al. found issues surrounding privacy were not a major concern for libraries, with only 14% of respondents stating they had a privacy policy, compared with 81% having an AUP and 64% having a data protection policy: “This suggests a hierarchy of priorities, with policy set out on issues where there is public anxiety (acceptable use) and where law makes it necessary (data protection), but with privacy as a broader ethical issue left to be addressed on an *ad hoc* basis” (Sturges et al., 2003: 48). They also noted that library staff did not place privacy as a high priority compared with other aspects of service when surveyed (Sturges et al., 2003).

3.9.2 Limits to privacy

A library patron who wishes to look up sensitive material in a book can easily take the book and sit in a quiet, secluded area of the library. Trying to hide the information displayed on a screen is much more difficult (Cottrell, 1999). This is echoed by Sturges et al.: “In the digital library, privacy from the librarian, or those who have access to library files, is less possible than it was in libraries of print” (Sturges et al., 2003: 45). The library now holds vast swathes of information contained electronically (Sturges et al., 2003) and new technology means new risks to patron privacy and confidentiality: “Although confidentiality is taken for granted in reference work, electronic communication increases the chance of inadvertent breaches” (Cottrell, 1999: 109). The ethical conflicts and decisions may be taken right out of the librarian’s hands. If a patron needs health information, the librarian can help by locating the best texts and information they know has been carefully selected, and at all times the librarian has the patron’s confidentiality in mind. When the patron tries to locate information on the Internet however, the situation changes: “The primary ethical responsibility lies with the developers and maintainers of the Web site not to misuse information gathered from registration screens. The ethical question for the library concerns the need to inform, educate, and, if necessary, caution the patron about Web usage” (Cottrell, 1999: 110).

Confidentiality is then out of the librarian's hands, and they have a dilemma: "The conflict, then, is between the responsibility to provide open access to new information mechanisms such as the Web and the responsibility to protect the confidentiality of the transaction" (Cottrell, 1999: 110). This heightened risk then gives the library staff "new responsibilities" (Cottrell, 1999: 109). Also, with the immense amounts of details contained on each and every user, Estabrook (1996) has argued that this should be put to use. So much data is voluntarily given out by consumers the library should take advantage to keep itself from being left behind: "For the most part, libraries provide searching tools that allow users to target their needs more effectively. Now we should exploit those tools to allow us to target users' needs more effectively" (Estabrook, 1996: 48). This consumer-driven aspect of the library is perhaps an ideal way to both encourage usage and keep the library current, however this also raises questions regarding patron privacy, changing user details into "a commodity rather than a confidential trust between professional and client" (Sturges et al., 2003: 85).

3.10 Ethical landscape and the Internet

Cottrell notes that in the 1990s in computing and philosophy new technologies opened up various discussions on whether ethical systems should change. The library sector however, was somewhat behind: "indicating that as we've been so busily keeping up with the technology, we may not have paused to consider the implications" (Cottrell, 1999: 107). Problems on the Internet are often exacerbated, with easier access to commit certain crimes and other indiscretions such as bypassing copyright restrictions. According to Hauptman and Motin (1994) however, the ethical landscape remains largely unchanged: despite the apparent ease of obtaining information online, the ethical principles which cover freedom of access, privacy etc., do not necessarily change just because the information is accessed through the Internet. Hauptman and Motin state that thinking in terms of anything other than general ethics and moral principles is useless and the world of the Internet does not have a special moral code all of its own: "Cyberethics and virtual morality are nonsense. They are particularly harmful if they allow us to confuse reality with a nonexistent universe where

unethical actions are permitted. The ethics of human interaction remain constant" (Hauptman and Motin, 1994: 8). What has been written before about moral philosophy and systems of ethics still stand the same on the web as they do in life, and the Internet should not change the way we act: "The situations have changed, but the principles or desired results remain the same" (Hauptman and Motin, 1994: 8).

Although the ethical landscape may remain largely unchanged, the potential threats to the landscape have evolved, as McMenemy notes: "There are fundamental values that information professionals stand to protect, and the reality is that some digital solutions to service delivery may challenge those values" (McMenemy, 2016: 3). For example, with technology there are new ways to monitor people, find people, and talk about people, and all of these threaten individual privacy (Nissenbaum, 2010). Being on the Internet can help individuals connect with one another, but it can also make them more exposed and thus vulnerable: "As connectivity increases access to information, it also increases the possibility for agents to act based on the new sources of information. When these sources contain personal information, risks of harm, inequality, discrimination, and loss of autonomy easily emerge" (Van den Hoven et al., 2016). Some of these directly affect the library user – electronic monitoring via key-logging or surveillance cameras for example – whilst other aspects such as social networks, where people can discuss other people without the person being aware, are areas the library professional can educate patrons on. However, with the chance of reaching more patrons through social networks and other new communication methods, the library may have to question how rigidly it wishes to stick to fundamentals of patron privacy, lest it be left behind in the technological landscape. The possibility of enhancing service delivery may lead libraries to collect data, however this would mean moving away from the library's image of a haven for privacy and freedom of expression (Zimmer, 2013). Poulter notes that technological advancements bring new challenges, thus the librarian must rely on the ethical principles they adhere to:

“As connectivity increases access to information, it also increases the possibility for agents to *act* based on the new sources of information… Although the Internet has changed how access to information in the public library is delivered, it has not changed the central elements of the librarian’s role” (Poulter, 2005: 206). (emphasis in original)

This is echoed by Cottrell: “even though information technology may result in more complex systems, the basic ethical commitments remain the same, and traditional ethical considerations are shown to apply to issues of privacy, confidentiality, and other aspects of networked communication” (Cottrell, 1999: 108). Zimmer (2010) states that the patron, and what they expect of the library regarding their privacy, is what the library should look to as a guide.

In academic libraries, Jones and Salo (2018) notes the use of data analytics to potentially improve student learning, and the potential ethical problems with its usage. In particular they note the use of learning analytics – measuring data about students to help improve the learning environment (Siemens, 2012 in Jones, 2017) – and the possible clash with the ethical prinicples of the library practioner: “Naturally, libraries want to use these data flows to their benefit and to that of their users, but at what cost?” (Jones and Salo, 2018: 310). Indeed, whilst the aims of this data-mining might be positive – such as improving education for students – there are concerns over the surveillance used during such practices, and the analysis of individuals’ personal information, potentially stifling intelluctual freedom (Jones, 2017). The use of such surveillance, coupled with the data potentially going out of the libraran’s hands is something many librarians are uncomfortable with (Hoel et al., 2018).

Jones (2017) however notes the potentially positive use of learning analytics, and also surveillance, for intellectual freedom. For instance, helping students to further their education by analysis of their search history, to offer more suggestions for reading. Noting that such use of technology neither restricts the student in terms of what they use in the library, nor does it constrict the student’s ability for freedom of expression, Jones states: “autonomy is protected, and internal desires are unaffected” (Jones, 2017: 8). However, Jones also notes

such uses of data will also need to be combined with rigourous policy and attention to student privacy (Jones, 2017). Likewise, Jones and Salo (2018) note that using data-mining like learning analytics requires library practioners to help shape the conversation and policy, if ethical principles are to be kept intact. The use of technology to help enhance the patron's information access can be positive, but requires a strict look at how it could potentially affect fundamental library values such as privacy and freedom of expression.

3.11 Conclusion

This chapter has given an overview of surveillance, including the metaphor provided by Michel Foucault of the panoptic principle, based on the institutional building designed for maximum productivity and control, with a heightened use of surveillance techniques by Jeremy Bentham. The panoptic principle and surveillance studies in general has become a large area of research, despite this there are only limited insights into the potentiality of using the panoptic principle within library and information science. Surveillance is a complex and often controversial subject. It is seen as a way of preventing crime, protecting citizens, as well as a method of spying and subsequently controlling populations.

This chapter has also given insight into the ethical issues in public library access, particularly around freedom of expression, access to information, and privacy, key aspects of the public library service. These issues become potential quagmires when balancing the individual user with the community the library service is there to serve. These issues can also become compounded when they are subjected to leaps in technology such as access to the Internet. Although the ethical dilemma may remain the same with or without cyberspace, the Internet, and the access it provides to new information, new communities, and new forms of scrutiny can have a major impact on how the library service deals with these issues. The library has the ability to enhance services for patrons, as well as make efforts to try and protect patrons from possible disturbing content through access management tools such as surveillance, filtering, and analysis of user data, however there is potential for this to become overbearing, and having a chilling effect, leading patrons to start self-censoring, which goes directly

against the library's fundamental principle of freedom of expression and access to information. This issue is further complicated because of the traditional stance of libraries regarding patron privacy. Allowing the use of patron data, and different types of monitoring could protect the library against facilities being used for nefarious purposes, as well as allowing the library to provide a more tailored and up to date service. Using such facilities however, may have library staff calling into question their ethical stance on patron privacy. Analysis of a document like the AUP – the main gateway to the use of ICT facilitates in the public library – examines how PLAs provide access to the Internet, and if this access provision is one that could potentially stifle freedom of expression and access to information, through the use of potential chilling measures such as over reliance on certain types of surveillance and filtering, as well as how these sort of measures are communicated.

In the next chapter, the research questions will be formulated, alongside a detailed overview of the methods to be used in this study.

4 Methods

4.1 Introduction and research questions

Following the literature review, it was clear that access management is an important part of public library Internet access, with filtering, surveillance, and AUPs as major yet often controversial parts of this process. These parts can both prohibit and promote information access in equal measure. Alongside this, the panoptic principle is a powerful metaphor in the complicated area of surveillance studies, one that has had little application to public library research. The nature of surveillance is complicated, having both disciplinary and protective elements. Lyon notes that surveillance is two-sided, with one side that is caring, and another that is controlling (Lyon, 1994; 2001). Ethical considerations are also seen as an important part of the information profession, that should be apparent in the AUP. The content of the AUP is an under-researched yet major part of managing access in the public library. With that in mind, three research questions were proposed:

- RQ1 In what ways does the public library AUP document reflect the panoptic principle?
- RQ2 How does the public library AUP encourage and discourage access to information and freedom of expression through surveillance, filtering, and commitment to ethical principles?
- RQ3 How effectively does the AUP balance the care and control elements of public access?

A mixed methods approach was decided upon: mixed methods research combines elements of both qualitative and quantitative methods in order to get deeper insights, substantiate findings, and gain an enhanced understanding of the research questions (Creswell and Plano Clark, 2007; Johnson et al., 2007; Tariq and Woodman, 2013). Data collection would be performed through Internet searching and FOI request. The methods decided upon were:

- readability testing

- qualitative content analysis

This research used a mixed methods approach, in an explanatory sequential design whereby the quantitative aspects of the research, the readability testing, was expanded upon by the findings of the qualitative content analysis (Bryman, 2012). In order to gain insight into how access management in UK public libraries operates, it was decided that AUPs across the UK would be analysed. First, the AUPs would be gathered, alongside authorship information, using a combination of online searching and FOI requests. The AUPs were then put through an online readability calculator. The research then used qualitative content analysis to analyse the AUPs, including comparisons of tone between the documents and the information received about the authorship that had been gathered by the FOI requests. The methods used are described in further detail below.

4.2 Using documents for research

The analysis of the AUP documents and their importance in the provision of public library services was decided as a fruitful area of research. Prior notes that documents are a dynamic and active part of social action but are often portrayed simply as "containers of facts" rather than important pieces of social reality in themselves: "Documents form a 'field' for research in their own right, and should not be considered as mere props to human action" (Prior, 2011: 26). Indeed, Pickford notes that documents are often used as supplementary or supporting information in information science research rather than being the main source of analysis (Pickford, 2013). Documents can be productive sources of data for researchers (Bryman, 2012). They can be deeply revealing as to the practices and beliefs of an organisation:

"Although documents are often presented as objective statements of social fact, they actually reflect the values and norms of the society or social group in which they are produced. Thus, such secondary data can give sociologists tremendous insight into the organisation of societies and cultures at particular points in time" (McNeill and Chapman, 2005: 147).

The study of documents gives “Important insight into the social meanings that underpin social action” (McNeill and Chapman, 2005: 155) and can tell “a great deal about the way in which institutions and events are constructed and the interactions and interpretations that shape these” (McNeill and Chapman, 2005: 156). Official documents in particular have specific advantages such as their formation not being initiated by the researcher themselves: “because they have not been created specifically for the purposes of social research, the possibility of a reactive effect can be largely discounted as a limitation on the validity of data” (Bryman, 2012: 542). There is no influence from the researcher on the nature of the information being analysed. AUPs are an important part of managing Internet access in public libraries, and these documents can reveal how the public library discusses ethical considerations such as privacy and freedom of expression, as well as how monitoring and subjects like misuse of the facilities are communicated to patrons. The AUP documents can reveal a lot as to the nature of each library service, and having been already produced prior to this study for the purpose of managing Internet access, they will have no external influence from the researcher.

4.3 Data collection

In the UK, public libraries are controlled by various types of local authority including: unitary authorities; metropolitan boroughs; London boroughs; Scottish local authorities; and Welsh local authorities. Authorities such as district councils do not control public libraries. In the UK there are 206 PLAs, as listed by CILIP’s directory *Libraries and Information Services in the United Kingdom and the Republic of Ireland* (CILIP, 2015). To conduct a comprehensive analysis of public library AUPs in the UK, it was decided that AUPs would be analysed from every PLA. Other studies that have analysed access management and AUPs have used surveys, discourse analysis, statistics, and case studies, but have not analysed the AUP content of the entire public library network of the UK. FOI requests were used to collect the data, to ensure that coverage was as full as possible, as surveys can have varying response rates (Bryan, 2012). Previous studies such as the MAIPLE project’s survey on access management to all 206 authorities had a response rate of 39% (Spacey et al., 2015: 74). In

2012 CILIP carried out a survey on issues such as staffing and budget cuts covering 174 authorities across Wales, England, and Northern Ireland, which garnered a response rate of 53% (CILIP, 2012).

AUPs were first collected from those available online. Each PLA creates its own AUP, meaning an AUP in one area of the UK will not be identical to another. Firstly, the authority website was found by a Google search, or by simply typing the authority name + gov.uk. The researcher navigated to the public library section of the website, and then browsed what was thought to be the relevant sections for the AUP, which was the 'Computers and Internet' section of the library pages, or the 'Policy Documents' section of the library pages. Like the AUP documents themselves, authority websites are designed at the local level. Therefore, although they did share similarities, navigating the website was not the same process from one authority to the next. If this method did not locate the AUP the researcher used the authority website's search function. If the AUP was not found by using the websites internal search function the researcher searched the authority website using the **site:** function on Google search. If the AUP was still not found the researcher submitted a FOI request for the AUP, using the email provided by the authority website, or the online form provided by the authority if an email address was not available. The researcher found the relevant FOI page on the authority website by using the website search function, the content pages, as organised alphabetically, or sometimes the FOI request hyperlink was located on the authority's home page. If the AUP could be located, it was downloaded, and then imported to the NVivo software suite. If the AUP could not be located, a FOI request was sent, asking first for a copy of the AUP, and then secondly, a question regarding its authorship. AUPs were requested to be presented preferably in a digital format, to ease transition to the NVivo software program for analysis. If the AUP could be located, an FOI request was sent only to determine the authorship of the document.

4.4 Freedom of information requests

In the UK, access to information is governed by the Freedom of Information Act 2000 (England, Wales, and Northern Ireland) and the Freedom of Information Act 2002 (Scotland). The Freedom of Information Act provides public access to information held by public authorities. It does this in two ways: public authorities are obliged to publish certain information about their activities; and members of the public are entitled to request information from public authorities. These public authorities include schools, the NHS, police, and public libraries amongst others. Following the date of receipt, the public authority has 20 working days to reply to the request, after which they must provide the information, refuse under one of the Act's exemptions, or ask for clarification or extension. Clarification may be sought if the applicant's request is not clear, or not specific enough regarding the information that they require. Requests must be made in writing (this includes electronic communication such as email).

Freedom to access information is a notion that is enshrined in both the *Universal Declaration of Human Rights* and the *European Convention on Human Rights*, and the Freedom of Information Act is seen as being a crucial part of democratic debate, allowing those not in academic positions to gain access to information about public institutions (Birkinshaw, 2001; Savage and Hyde, 2014). Anyone, including non-UK citizens and organisations such as newspapers may request information and they do not have to justify their reasons for doing so. On this latter point the Information Commissioner's Office (ICO), which is the independent authority set up to uphold information rights in the UK, states that: "an applicant (requester) does not need to give you a reason for wanting the information. On the contrary, you must justify refusing them information" (ICO, 2017: 5).

FOI requests are an ideal collection method for documents held by local authorities (Savage and Hyde, 2014: 308). They are helpful for obtaining large amounts of data about different authorities: "FOIA requests are particularly useful where comparisons are sought to be drawn between various public authorities. By using a standardised FOIA request, data

obtained from public authorities can be standardised" (Savage and Hyde, 2014: 309). Savage and Hyde note the importance of the Freedom of Information Act for researchers: "FOIA requests have great potential on both theoretical and practical levels. Practically, the FOIA requests allow researchers to access data that they wish to subject to analysis. Theoretically, data obtained through requests can be seen as a powerful tool for democratising the research process" (Savage and Hyde, 2014: 304). The Freedom of Information Act is a powerful tool for research, as it is not bound by ontological or epistemological research paradigms (Savage and Hyde, 2014), and it allows information that would previously have been difficult or impossible to gather much easier, allowing for information to be much more publicly available, dispensing the need for special access permits (Almond, 2008; Savage and Hyde, 2014). Despite its potential usefulness, and the ease with which one can use it, using the Freedom of Information Act for research purposes is not widespread, particularly in areas such as social science (Brown, 2009). Savage and Hyde note that researchers often focus on the negative aspects of the Act rather than its usefulness (Savage and Hyde, 2014: 303).

4.4.1 Submitting the FOI request

Submitting the FOI requests was a relatively straightforward process, although sometimes there were delays in submitting the request; one authority did not allow the researcher to complete the webform because the postcode being used was not recognised, another authority had the wrong email address displayed on its FOI request information page. Whilst the use of a standardised FOI request helps to standardise the replies, the use of FOI does have to rely on the answers provided by the requested authority (Brown and McMenemy, 2013). To allow for potential problems Savage and Hyde (2014) note that it is useful to conduct a test sample, if the FOI is to be applied on a large-scale. Both FOI requests were tested to a small number of authorities first (ten for each) before sending them to all 206 PLAs. The test FOI requests were as follows:

- Q1: I am seeking a copy of the Acceptable Use Policy made available for users of computer facilities in public libraries in your local authority, preferably in electronic format, sent to this email address: [NAME REMOVED]
- Q2: I would like information as to who was involved in writing the Acceptable Use Policy made available for users of computer facilities in public libraries in your local authority, preferably in electronic format, sent to this email address: [NAME REMOVED]

Whilst the first question had no issues, it was clear for the second question that by asking "who was involved" made it seem as if the FOI request wanted the names of the individuals involved, which was not the case, and also could be refused under the Data Protection Act. Thusly, Q1 was kept the same for the remaining authorities, and Q2 was changed to the following:

- Q2: I would like information as to which departments were involved in writing the Acceptable Use Policy for users of computer facilities in public libraries in your local authority, preferably summarised in electronic format sent to this email address: [NAME REMOVED]

After this, there were no issues regarding Q2. Two of the authorities provided the staff AUP instead of the public one, and two authorities queried which policy the FOI request referred to (some authorities term the AUP "Conditions of Use" for example). The researcher followed up these replies to ensure the correct AUP was provided.

4.4.2 Handling replies

Savage and Hyde note that the use of FOI requests can generate large volumes of data, "particularly if the same request is submitted to a large number of authorities" and that it is important to "anticipate the handling of this data in the research design" (Savage and Hyde, 2014: 309). For this research, each response was routed to a different email folder dependent upon the nature of the reply. Usually, the public authority would respond with an initial email acknowledging the request, and would also outline a timeline for their response.

This would be stored in a sub-folder to the inbox. The follow-up email was then stored in a different sub-folder. An external checklist was also made in Excel detailing dates sent and received to keep track of replies.

4.5 Authorship

Alongside the AUP itself, an FOI request was used to gain information regarding the formation of the AUP. Authorship information was sought to determine how AUPs differed depending on who was involved in its creation; for example, if AUPs that are heavily negative in tone, or especially difficult to read are correlated with certain types of author. Also, it was important to find out how much input library staff had over the AUP's formulation and if the lack of staff involvement is reflected in the AUP after the qualitative content analysis was performed.

Authorship information was stored in a spreadsheet detailing the following information:

- **Name**: the number assigned to the AUP
- **Length of time to reply**: how long the authority took to provide the information
- **Whether the information was provided**: this was a simple yes or no
- **Whether the reply required extra days**: this included how many extra days were required
- **Reasons for the delay**: this included replies being sent to the wrong address, and requests for clarification from the authority
- **Who wrote the AUP**: all of the parties mentioned
- **Consultancy information**: some of the replies noted that there was input from other departments
- **Approval information**: some authorities stated the AUP was signed off by a senior figure
- **Other details**: anything else provided by the authority. This included details of research that went into the AUP such as using CILIP guidelines or help from other libraries for example

4.6 Readability testing

Once all the AUPs were gathered, they were analysed using online readability testing software. Readability is defined as how easy a piece of writing can be read and understood (Grewal et al., 2012). Readability is a significant aspect of writing; it impacts the understanding of a text (Badarudeen and Sabharwal, 2010: 2572), and this becomes a more important principle the more general an audience is (Klare, 2000). Readability will also, in part, determine how useful a text is, especially in the field of technical texts such as manuals (Smith and Kincaid, 1970). For a policy document such as the AUP in the public library, it is essential that it is designed for a variety of readers, who will be at varying levels of literacy. As Seely observes: “It is safest to assume little or no prior knowledge of your subject, unless you have good reason to believe otherwise. Far more people have been put off reading a text because they could not understand it than because they were offended at being treated like idiots” (Seely, 2013: 124). Those who use their local library will differ vastly in age, education, and reading ability, thus the public library’s AUP must serve a variety of people.

In a survey of epilepsy information websites and their readability, Brigo et al. note that having the information available is not enough; the information made available must also be understood by the reader (Brigo et al., 2015: 35). The same principle applies to the library AUP; it is not enough for the policy to simply exist, it must be clear and intelligible to those it was written for. Furthermore, as a contract and a “quasi-legal” (McMenemy, 2014: 1) document, it is essential that the AUP is written in such a way as to be clearly understood by the patron. The AUP is for educating users as well as protecting the library service from misuse, therefore readability is a key part of making the document successful: if an AUP is not easily read by the patron, any information it holds will be unclear leaving the patron in the dark about what the service offers and how to take advantage of it, and any violations of UK law the patron commits can be potentially waived away by pointing to the incomprehensibility of the document. There is also the ethical issue of providing users a difficult to understand document that they must accept to gain access to the facilities. An important principle of

public library service is supporting access to information. An AUP that is difficult to understand will not facilitate this.

A person's reading ability is usually dependent on how much education they have received (Bluman et al., 2009). The National Literacy Trust note that around 5.1 million adults in England are functionally illiterate (National Literacy Trust, 2017a), and a 2011 survey of the literacy, numeracy and ICT skills of those aged 16-65 in England by the Department for Business, Innovation, and Skills recorded that:

- 5% achieved Entry Level 1 (National School curriculum equivalent for attainment age 5-6) or below (approximately 1.7 million people). Adults below Entry Level 1 may not be able to write short messages to family or select floor numbers in lifts.
- 2.1% achieved Entry Level 2 (National School curriculum equivalent for attainment age 7-9) or below (approximately 730,000 people). Adults with below Entry Level 2 may not be able to describe a child's symptoms to a doctor or use a cash point to withdraw cash.
- 7.8% achieved Entry Level 3 (National School curriculum equivalent for attainment age 9-11) (approximately 1.7 million people). Adults with skills below Entry Level 3 may not be able to understand price labels on pre-packaged food or pay household bills.

(Department for Business Innovation and Skills, 2011: xxvi-xxviii).

Readability testing is widely performed on health materials, such as the quality of healthcare information available online (Agarwal et al., 2013; Svider et al., 2013; Hansberry et al., 2014; Best et al., 2015; Brigo et al., 2015); health information leaflets and documents, including consent forms (Hedman, 2008; Walters and Hamrell, 2008; Kasabwala et al., 2012; Eltorai et al., 2015; Graham et al., 2015; Corcoran and Ahmad, 2016); and health education (Lee and Belden, 1966). It has also been used for reports in other areas of science, such as forensics (Howes et al., 2013; 2014a; 2014b), and also for business management (Lo et al., 2017). In

the case of the library and information science profession, however, research into the readability of materials and documentation in the library – such as policy documents like the AUP – is limited. Readability testing studies have been conducted with regards to student research (Gray, 2012) and university library websites (Muswazi, 2009; Lim, 2010). A comprehensive but easily read AUP is encouraged and promoted by library groups (CILIP, 2011; ALA, 2012). However, readability testing is not actively practiced in the profession.

AUPs were supplied as a mixture of Word documents, PDFs, and image files. Several of the AUPs were not actually text but rather images, with text appearing in a boxed area, unable to be "read" by readability calculators. The text was extracted from these using Microsoft OneNote 2016's Optical Character Recognition (OCR) tool on a Windows 10 computer, and then checked manually by the researcher to make sure they were complete and that the text had been successfully transferred over during extraction. AUPs were then put through four readability tests (Flesch Reading Ease, the Coleman-Liau Index, the Gunning Fog Index, and the SMOG (Simple Measure of Gobbledegook) Grade), using the readability testing website: readable.io (previously readability-score.com). The AUPs were uploaded to the readable.io website which processed the files and gave the subsequent results as an Excel spreadsheet. These were then combined into one large spreadsheet for analysis. A total of 205 out of a possible 206 AUPs were collected (99.5%), along with 172 responses for the authorship question (83.5%).

4.6.1 The readability tests

The four readability tests used for analysis were the Flesch Reading Ease, the Coleman-Liau Index, the Gunning Fog Index, and the SMOG Grade. The four tests use a combination of word complexity, polysyllabic word count, character count, and sentence length to calculate the readability of a piece of text, with the specific formulas utilised in each test presented in the table below:

Table 1 Readability formulas (from readable.io)

READABILITY INDEX	FORMULA	OUTPUT
FLESCH READING EASE	206.835 - (1.015 x ASL) - (84.6 x ASW)	Index Score
	where ASL = Average Sentence Length (words divided by sentences)	
	and ASW = Average Syllables per Word (syllables divided by words)	
GUNNING FOG INDEX	0.4 (ASL + PHW)	US Grade Level
	where ASL = Average Sentence Length (words divided by sentences)	
	and PHW = Percent Hard Words (words of 3+ syllables divided by words)	
SMOG GRADE	√ (total polysyllabic words x [30/total sentences]) + 3	US Grade Level
COLEMAN-LIAU INDEX	0.0588 L - 0.296S - 15.8	US Grade Level
	where L = average number of letters per 100 words	
	and S = average number of sentences per 100 words	

These four readability tests were chosen to undertake this analysis because they are among the most commonly used and well-known of the readability formulas (Kondilis et al., 2010; Svider et al., 2013; Kugar et al., 2017). Specifically, the Flesch Reading Ease test was selected because of its accuracy and simplicity (Kondilis et al., 2010; Rudd, 2010). The SMOG Grade test is both widely used and considered to be a very reliable instrument of measuring readability (Hedman, 2008; Fitzsimmons et al., 2010; Kondilis et al., 2010; Rudd, 2010; Best et al., 2015) and has been found to be consistent performance-wise (Wang et al., 2013). The Coleman-Liau Index was also selected for its consistency (Vargas et al., 2014). The Gunning Fog Index was selected because of its frequency of use, especially in regards to information materials concerning health and medicine (Luk and Aslani, 2011; Hamnes et al., 2016).

4.6.1.1 The Flesch Reading Ease

Developed by writing researcher Rudolf Flesch, the Flesch Reading Ease test works by measuring average sentence length in words and average word length in syllables. Flesch wanted a scientific method to help create effective working text (Longo, 2004). The output is a score from 0-100 with higher scores indicating an easier level of readability. Table 2 reflects the difficulty of scores and corresponding literature types, adapted from Flesch's own calculations (Flesch, 1948). The higher the score is, the easier the readability of a piece of text. Scores of 60-70 indicate that the text should be understandable by those aged 13-15 years old (Grewal et al., 2012).

Table 2 Flesch literature types

Score	Typical Magazine	Difficulty
0-30	Scientific	Very Difficult
30-50	Academic	Difficult
50-60	Quality	Fairly Difficult
60-70	Digests	Standard
70-80	Slick Fiction	Fairly Easy
80-90	Pulp Fiction	Easy
90-100	Comics	Very Easy

The remaining three tests all output a corresponding US school grade level, a breakdown of which can be found in Table 3, along with reflective age numbers.

Table 3 US grading system and corresponding ages

Grade	Age Range
1st	6-7
2nd	7-8
3rd	8-9
4th	9-10
5th	10-11
6th	11-12
7th	12-13
8th	13-14
9th	14-15
10th	15-16
11th	16-17
12th	17-18

4.6.1.2 The Gunning Fog Index

The Gunning Fog Index was conceived by the college textbook publisher, Robert Gunning in 1952 in an aim to make writing easier for readers, as a lot of written material is full of fog – too many lengthy words and sentences (Cantore and Passmore, 2012; Seely, 2013). The Gunning Fog Index relies on sentence length and syllables, with “foggy” words being 3 syllables or more. The Gunning Fog Index grades text, with higher scores indicating a higher level of reading difficulty. A rating of 7 or below should be understood by schoolchildren, those of about 15 should be able to understand text at level 10, and a score of 12 or higher indicates university level or above (Cantore and Passmore, 2012; Seely, 2013). Text should aim for a score of 7-8, with anything over 12 becoming too difficult for a general audience (Grewal et al., 2012: 1463).

4.6.1.3 The SMOG Grade

The SMOG Grade test works by selecting sentences from the beginning, middle and end of a piece of writing, and counting the number of words in each that contain 3+ syllables, designed to be a simple yet strong test (McLaughlin, 1969; Fitzsimmons et al., 2010). A score of 13 or over requires the reader to have received college or university education, 17 or over requiring graduate training, and anything over 19 a higher professional qualification (McLaughlin, 1969: 645). For a general audience, the National Literacy Trust recommend that writing should have a SMOG score of about 10 (National Literacy Trust, 2017b).

4.6.1.4 The Coleman-Liau Index

The Coleman-Liau Index, developed by Coleman and Liau in 1975, relies on characters rather than syllables per word in order to be easier and more economically feasible for large organisations such as the US Department of Education, with the resulting calculation outputting a US Grade level (Coleman and Liau, 1975). Like the Gunning Fog Index and the SMOG Grade readability formulas, the lower the Coleman-Liau Index score is, the easier the writing should be to read. A score of 14 equates to college sophomore or 2nd level

undergraduate (about 19-20 years old) (Wong and Levi, 2016). Standard writing should aim for a score of 7-8 in this test (Wilson et al., 1997).

4.6.2 Readability scores of a selection of texts

To provide some contextual comparison to the AUP results, three other pieces of writing were also tested. These were:

- a 2016 article about quantum computing from the magazine *The New Yorker*
- the Terms and Conditions for using Apple's iTunes software
- a BBC News website profile of opal mining

These three texts were thought to represent a variety of difficulty levels and could be contrasted with the AUP results for comparison. The website of the BBC is designed to be consumed by a mass audience, *The New Yorker* magazine provides a serious, in-depth read of often more difficult subjects, and even though the terms and conditions for iTunes is supposed to be designed for a large user-base, it has been described as almost impenetrable for the average reader (Pidaparthy, 2011; Hern, 2015; Kamen, 2015). The scores for the three texts are shown below, in Figure 1 and Table 4.

Figure 1 Readability scores of a selection of texts

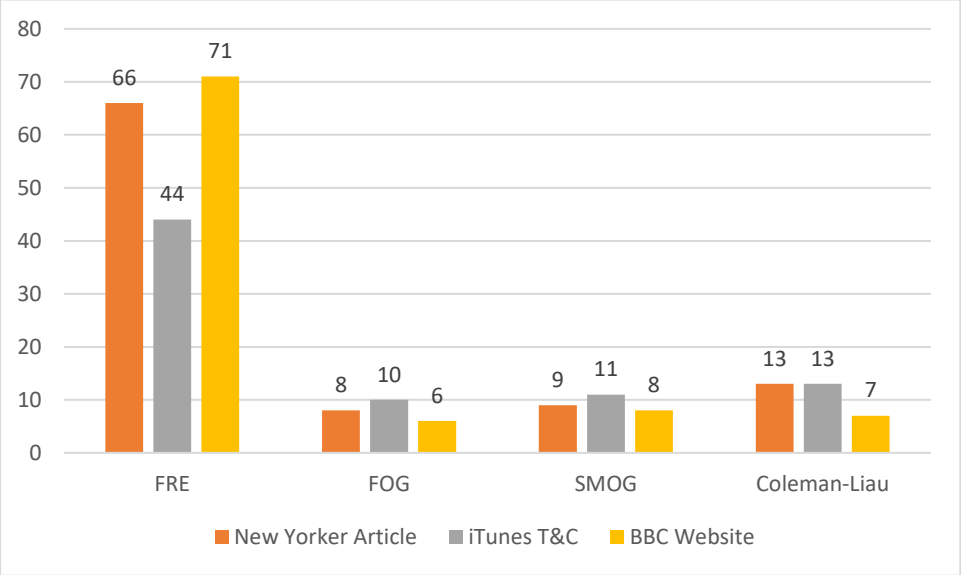


Table 4 Readability scores of a selection of texts

Text Types	FRE	FOG	SMOG	Coleman-Liau
New Yorker Article	66	8	9	13
iTunes T&C	44	10	11	13
BBC Website	71	6	8	7

The BBC News website, aimed at a wide audience, scores at easier levels across all four tests by a considerable amount. As expected, the article from *The New Yorker*, and the terms and conditions for iTunes both scored at higher levels of difficulty, particularly the iTunes document.

4.7 Qualitative content analysis

4.7.1 The importance of language

Fairclough notes that with an increasing reliance on knowledge in the economy, language and communication is becoming more and more important in our lives. This focus on language and its use has led to "more conscious attempts to shape it and control it to meet institutional or organisational objectives" (Fairclough, 2001a: 231) and "in broad terms, language has become more salient and more important in a range of social processes" (Fairclough and Wodak, 1997: 259). In particular, the study of power is intimately linked to the study of language: "nobody who has an interest in relationships of power in modern society, can afford to ignore language" (Fairclough, 2001b: 3).

Qualitative content analysis is accepting of the constitutive nature of nature of language, allowing for an interpretative approach and, like discourse analysis, the meaning of such language is "not immutable, but that it is constructed in the context of the questions asked of it" (Williamson et al., 2018: 461). Likewise, Krippendorff states that "content analysis rarely aims at a literal description of communications content" (Krippendorff, 1989: 404). Krippendorff notes the importance of communications:

“Communications, messages, and symbols differ from observable events, things, properties, or people in that they inform about something other than themselves; they reveal some properties of their distant producers or carriers, and they have cognitive consequences for their senders, their receivers, and the institutions in which their exchange is embedded” (Krippendorff 1989: 403).

As an unobtrusive method, qualitative content analysis can be applied well to written data, with each document being given the same attention (Krippendorff, 1989, Mayring, 2000; Gbrich, 2007; Bryman, 2012). Qualitative content analysis is particularly suited for documents such as the AUP for it can give insights into an individual or an organisation’s attitudes, values, and prejudices (Krippendorff, 1989: 404), and analysis can be done on both the latent and manifest level (Hsieh and Shannon, 2005).

Qualitative content analysis is described by Hsieh & Shannon as “a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns” (Hsieh and Shannon, 2005: 1278). Content analysis can be applied to both quantitative and qualitative data, and can be either inductive, deductive, or both (Elo, S. and Kyngäs, 2008; Vaismoradi et al., 2013). In content analysis, measurement “consists of counting the occurrences of meaning units such as specific words, phrases, content categories, and themes” (Weber, 1990: 70). Content analysis is a “systematic coding and categorizing approach used for exploring large amounts of textual information unobtrusively to determine trends and patterns of words used, their frequency, their relationships, and the structures and discourses of communication” (Vaismoradi et al., 2013: 400). Qualitative content analysis allows for both manifest and latent aspects of language to be explored, whilst also allowing the more quantitative aspects of content analysis such as frequency counts (Hsieh and Shannon, 2005). Qualitative content analysis allows for frequency counts as used in quantitative content analysis, however also allows for these counts to be analysed by using a qualitative approach (Mayring, 2000; Gbrich, 2007). Codes may be initially pre-defined through the literature

review, guided by the research questions, but there is also reflexivity, with codes appearing iteratively as the researcher works through the documents (Bryman, 2012), with the aim to be “systematic and analytic but not rigid” (Altheide 1996: 16).

The stages of qualitative content analysis carried out for this study are detailed below, and are based on Zhang and Widemuth (2016).

Step 1: Preparation of data.

Data must be prepared for the researcher’s needs for analysis. Qualitative content analysis can be used on various types of data, but data needs to be in a format that is conducive to analysis; most often, written text. Which texts are to be analysed will be generated from what the researcher wants to find out. (If the data comes from existing texts, the choice of the content must be justified by what you want to know (Patton, 2002).) Deciding what to sample should be based on what the researcher wants to find out, and how much time is available to them for research (Bryman, 2012).

In this case, deciding which texts were to be used for analysis was relatively straightforward. The researcher’s interests were drawn to the public library AUP and the content within them. As mentioned in the data collection section, there are 206 PLAs in the UK and it was decided, to get a thorough and more reliable result, that data analysis should be performed on (ideally) all 206 AUP documents. As mentioned in the data collection section, the researcher managed to gather 205 out of a possible 206. Because of the data types used, that is, documents, preparing the data for analysis was straightforward. Texts were imported into NVivo for analysis. As mentioned in the readability section, some of the AUPs received were in image format, and therefore text was extracted using the OCR tool in Microsoft OneNote, then copied over to a Word document. More details on using NVivo as an analysis tool is provided in section 4.9.

Step 2: Defining the unit of analysis.

The units of analysis for this study were the themes derived from the literature review, with each individual AUP being the unit of examination in which to apply codes. Again, the texts under examination for this study made this stage straightforward, as they are already separate entities. This method differentiates qualitative content analysis from quantitative content analysis in that themes can be expressed in large or small instances, and texts of varying sizes can be coded accordingly. This way also allows for codes to overlap over texts (i.e. one text could be assigned to different coding categories) (Tesch, 1990; Figgou and Pavlopoulos, 2015).

Step 3: Develop Categories and a Coding Scheme

Zhang and Wildemuth state that categories can be derived from three sources: the data, previous related studies, and theories, and that coding schemes can be developed both inductively and deductively. For this research, there was a deductive, bottom-up approach to generating the codes. The themes were theory-driven, informed by the literature review. Qualitative analysis such as this will always have a degree of interpretation, however this can be mitigated by providing the coding framework for clarity (Bryman, 2012). The themes are detailed below, in section 4.8, and the coding framework is presented in Appendix 1.

Step 4: Testing the coding scheme on a sample

Prior to embarking on an analysis of all the AUPs used in PLAs across the UK, a pilot study was conducted in order to test the themes planned for the qualitative content analysis. Pilot studies are an invaluable means of testing one's research (Bryman, 2012), and due to the large number of potential AUPs to be used in the main study (206 authorities) it was decided a pilot study would be helpful in order to test current themes, and identify possible future themes. The pilot study was conducted on a dataset of 30 AUPs from public libraries across the UK.

Firstly, the data was collected by the researcher. 30 AUPs from the researcher's previous project were used for data analysis. These 30 AUPs had been found previously by using a

search engine (Google) to find available AUPs from across the UK. The first 30 positive results were selected for randomisation.

As well as the information regarding panopticism and care and control, the pilot study also highlighted other interesting aspects of the AUPs. The length of the AUPs varied widely – what was one AUP telling users that another was not? It was decided to keep an eye on the varying lengths of the AUPs, and what sort of omissions occurred between AUPs. Initially the researcher considered page counting the documents however due to formatting and design of the AUPs, having a longer set of pages does not necessarily follow that the document has more words. Along with the readability scores, the readability testing software used by the researcher also gave a word count output, meaning the researcher could compare the word count of the texts.

Step 5: Code the text

Once the pilot study was complete, the researcher carried out coding on all of the AUPs. Firstly, the researcher familiarised herself with the text. Each AUP was read through a number of times to gain familiarity. Coding was done by a close-reading of each AUP, going through each document line by line and marking the codes.

Step 6: Checking the coding

This step allows for the researcher to go back and check that the coding has been carried out satisfactorily. This step also allowed for the creation of extra codes pertaining to filtering. When it was clear some AUPs did not explicitly mention filtering, yet later alluded to blocked webpages, this became a new code. Likewise, when AUPs discussed eligibility for using the library service, only some were describing it in a full way, which lead to the creation of the eligibility partial code.

Whilst checking the codes, notes were taken down of some of the most interesting findings to be used when presenting the research report. This was done using the Microsoft Notepad programme.

Step 7: Drawing conclusions

At this point, the researcher starts to make sense of the identified themes, finding links, and exploring common patterns and trends. The use of the note-taking, as mentioned in step 6, was helpful in aiding this process.

Step 8: Reporting

To present the findings, selected examples were used from the data, to help give a deeper understanding to the interpretation of the data. The results and discussion are provided together in the next chapter (5).

(Zhang and Wildemuth, 2016).

4.8 Themes

The researcher worked out which themes to use for coding the documents in NVivo. The process was theory-driven, with codes derived from the literature review. This section will detail the themes used, and why they were chosen. The coding framework is included as Appendix 1.

Under panopticism and Lyon:

- **monitoring control**
- **monitoring care**
- **monitoring neutral**
- **not monitoring**
- **panoptic gaze**
- **general care**
- **general control**
- **compliance**
- **discipline (sanctions and banning)**
- **display of power**

Monitoring is a key component of panopticism. Lyon's themes of care and control were chosen as Lyon is a leading researcher in the field, and the usage of surveillance as both a caring and controlling mechanism is widely exhibited in the literature review. Lyon defined caring surveillance as that which protects and enables; the sort of surveillance that benefits the object of surveillance. Lyon defined controlling surveillance as the type of surveillance that is proscriptive and constrains the object. Lyon uses this example:

"I may ask you to 'watch over' my child to ensure that she does not stray into the street and risk being hit by a car. In this case, I have protection primarily in mind so that the child is shown care in a context where she can flourish. Or I may ask you to 'watch over' the same child to ensure that she does not get up to mischief. Now I am appealing to moral criteria, where other elements enter the picture, to do with direction, proscription, perhaps even control. The same process, surveillance – watching over – both enables and constrains, involves care and control" (Lyon, 2001: 3).

If the surveillance is caring it is being used to protect or enhance a patron's experience at the library. Text was coded as monitoring control if surveillance was being used to curb certain behaviours or to ensure patrons were abiding by rules. The controlling, proscriptive side of surveillance suggests regulating behaviour and points to panopticism. As well as the themes of care and control, text was also coded for neutral monitoring if surveillance was being carried out, but to no particular clearly defined end and to gain a sense of how many AUPs discuss monitoring in a neutral, rather than caring or controlling way. The node not monitoring was also used to find out if any library services do not use any form of monitoring as an access management tool.

Key to the panoptic principle is the unknown watcher. The idea that someone may be watching, but those under surveillance do not know at any one time if they are being watched or not. Text was coded as panoptic gaze if it suggested unverifiable surveillance.

As well as coding for monitoring care and control, text was also coded for general references to the themes of care and control to get a better sense of how AUPs were written in terms of being protective towards patrons or supporting them, or if they exhibited regulatory, governing aspects.

The notion of compliance is a key aspect in the functioning of the panoptic machine. Text was coded as compliance if it referenced following rules, or if something was framed in such a way as to compel a person to follow rules. Specific words such as “abide”, “obey”, and “comply” itself were also prompts for coding using the compliance node.

Discipline is an important concept in Foucault’s works, with the Panopticon being the pinnacle of the disciplinary institution: the subject becomes self-regulating. Text was coded as discipline if text discussed punishment, sanctions, or banning patrons.

The notion of power is key to how the Panopticon functions. Displays of power and authority can be detrimental to the patron if it stifles their freedom of access. How power is discussed is a key aspect of examining power relationships in the AUPs.

Under Sturges’ recommendation for the AUP (from Sturges (2002)):

Sturges created his recommendations by studying a number of other recommended criteria and reviewing the literature of what constitutes the ideal AUP. There are other recommended criteria, as noted in the literature review, Sturges’ list represents an overview of the literature, and is designed in particular for AUPs in the UK.

- **aims and objectives**

Sturges states that the AUP needs to begin with reasons for why the service is there, and what it is hoping to accomplish.

- **eligibility**

Who is able to use the service and if there are any special conditions (children requiring permission from their legal guardian for example) needs to be established. As noted

previously, when going over the documents initially it was clear that eligibility was discussed in an inconsistent manner and so the node of eligibility: full was also added for those AUPs that described eligibility requirements in a comprehensive way.

- **scope**

It should be stated what sort of use of the facilities may be used in the library – whether personal or study use only and if there are limitations on these services such as filtering software, or if certain services are restricted such as accessing chat rooms or gaming websites.

- **unacceptable use**
- **illegal use**

Sturges states that both illegal and unacceptable use must be mentioned in the AUP, such as copyright restrictions, uses pertaining to the Computer Misuse Act, and also uses that may be disturbing to other patrons.

- **service commitments**

What levels of service the library provides should be mentioned in the AUP. Disclaimers such as those pertaining to the legitimacy of information online may be mentioned.

- **user commitments**

Sturges notes that the library should state what it requires of the user, this may include accepting sanctions and what to do if the user wishes to appeal these.

Under filtering:

- **filtering in use**
- **filtering levelled**
- **filtering children only**
- **filtering not in use**

- **filtering not mentioned**
- **filtering unclear**
- **unblocking information**
- **efficacy**

Filtering is an important part of managing access in public libraries and how it is used and described can help or hinder a patron's experience at the library. Sturges notes the importance of notifying patrons regarding limitations on access, including the use of software such as filtering. There were separate codes for whether filtering was stated as being at different levels dependent on the type of user; if it was used exclusively for children's access, or if it simply stated it was being used and did not mention any type of delineation in terms of the different age groups.

Documents were coded as not mentioned if there were no mentions of filtering in the document. Documents were coded with the unclear node if filtering was being used but was not mentioned explicitly by the AUP.

Text was also coded for mentions of filtering software's efficacy. Part of being transparent in an AUP and allowing for fuller freedom of access indicates that the document should explain the reliability issues with such software.

Along with this, text was also coded if there were any guidelines present in the AUP as to how to unblock websites that may have been erroneously blocked, or how to alert staff if a filter has not blocked a site correctly.

CILIP's Ethical Principles:

Ethical considerations are an important part of the library and information profession. Judgements and balances have to be made regarding freedom of expression and privacy, alongside protecting the community and using access management facilities such as filtering. CILIP is the library and information association of the UK and their *Ethical Principles* document was used for these nodes.

- **Concern for the public good in all professional matters, including respect for diversity within society, and the promoting of equal opportunities and human rights.**
- **Concern for the good reputation of the information profession.**
- **Commitment to the defence, and the advancement, of access to information, ideas and works of the imagination.**
- **Provision of the best possible service within available resources.**
- **Concern for balancing the needs of actual and potential users and the reasonable demands of employers.**
- **Equitable treatment of all information users.**
- **Impartiality, and avoidance of inappropriate bias, in acquiring and evaluating information and in mediating it to other information users.**
- **Respect for confidentiality and privacy in dealing with information users.**
- **Concern for the conservation and preservation of our information heritage in all formats.**
- **Respect for, and understanding of, the integrity of information items and for the intellectual effort of those who created them.**
- **Commitment to maintaining and improving personal professional knowledge, skills and competences.**
- **Respect for the skills and competences of all others, whether information professionals or information users, employers or colleagues.**

4.9 Use of computer assisted qualitative data analysis

Qualitative content analysis was conducted using the NVivo software program. NVivo is a qualitative data analysis software package used to both organise and analyse data. Using computer-assisted qualitative data analysis (CAQDAS) to code documents, rather than doing so by hand was seen to be the most efficient way of analysing the AUP data. NVivo is especially useful when large amounts of data are being analysed (Pickford, 2013). The

researcher's experience with such software before, alongside the voluminous nature of the data to be analysed, and the ease with which one can organise data in NVivo in one place, made NVivo the ideal software to use. Using a CAQDAS tool has been noted to make the coding process faster, more transparent, and also can lend illumination on connections between data pieces that may previously not have been considered by the analyst (Bryman, 2012).

NVivo is a piece of software that allows the user to code information within documents under different themes which NVivo terms nodes. NVivo 11 defines a node thusly: "A node is a collection of references about a specific theme, case or relationship" (QSR International, 2015). Research is undertaken by using nodes to code the data. Text is selected, and saved to a particular node. Nodes can then be opened, and each piece of text saved to this node will be displayed. Single words, sentences, or whole sections of a document may be coded in NVivo. The different nodes can be arranged in a hierarchical manner if so desired and each node may be accompanied by a description. NVivo can reflect the percentage of a document that has been coded at a particular node. Documents can be viewed to highlight all pieces of text coded to particular nodes. The use of NVivo allowed for nodes to be changed or deleted if the researcher wished. NVivo allows for the importation of multiple file formats including pdfs, docs, images and sound files. This was ideal for this research as the AUPs were provided in a variety of text formats and also images.

The first step was reading through each document to get a general overview of each AUP, whilst taking note of general observations about each AUP, as suggested by Bryman (2012). Bryman (2012) suggests coding data as it is being collected, to help getting to grips with data, as well as easing into the data (if analysis is left until all data has been collected, this can feel overwhelming). The NVivo program facilitates this easily. The process of coding, viewing, and importing documents can be done simultaneously. Because documents are imported and stored in the main tray, the original documents can be accessed throughout the process. There are concerns that the usage of such software can fragment the text,

particularly in the case of interview transcripts where narrative flow is an important aspect of analysis and interpretation and fragmentation may result in a loss of these abilities (Bryman, 2012). Thus, the researcher made sure to be aware of the AUP document as a whole, and constantly referred back to it. Annotations allow for notes and observations within the text, which can be linked to both sources and nodes. Memos also allowed for observations and emergent ideas to be stored. Both of these allowed for ideas and observations to be noted down, without disrupting the flow of the source text. Memos were used frequently to capture extra information about both sources and nodes – for example commonalities between sources, and extra information about nodes, including information about possibly discarding or integrating nodes. One of the main benefits of using NVivo is the ease with which data is stored, coded, and manipulated. All documents are stored in one place, and text is coded without having to manually move sections of text around into the correct categories, or highlighting and annotating documents, losing the flow of the text. Once a text string is coded to a certain node, the researcher can view the document as originally presented, view the node and what text has been coded to it, or view the document with different nodes highlighted. Intersecting nodes can also be viewed in NVivo. The researcher found that being able to quickly go between different nodes and sources, allowed for familiarity with different sources to come easily.

Another advantage of NVivo over manual based coding was the use of functions. The researcher made the use of the ‘Query’ function in NVivo, including text searches and word frequency queries. Such functions would be difficult if the researcher was not using a CAQDAS program. Text can be searched and displayed by occurrence. The researcher can easily find out how often words appear in the documents as well as finding out which of the documents do not feature certain nodes. The text search function was used to find out how frequently certain words were used such as “compliance”, “prohibited”, and “abide”, appeared.

There are concerns that by using CAQDAS programs, the researcher becomes detached from the findings and the process becomes automated (Kelle, 1995; Smith and Hesse-Biber, 1996; Bringer et al., 2004; Bryman, 2012). The researcher found no problem with detachment, as the documents were re-read a significant number of times and this helped the researcher become more familiar with the documents. The researcher was aware of possible detachment from the data so made sure to look at texts as a whole, and not just as fragmented codes. Also, each document was read through more than once prior to the process of coding to ensure familiarity. Coding was all done by the researcher, and the researcher did not use the auto-coding function to retain involvement and attachment to the text. Whilst the software eases the process of performing qualitative analysis, it does not make the process self-generating, or decomplexifies the process: “The researcher must still interpret, conceptualize, examine relationships, document decisions, and develop theory. The computer can assist in these tasks but by no means does the computer analyse qualitative data” (Bringer et al., 2004: 249). The interpretive task is still up to the researcher, but the administrative aspect is performed by the software, instead of the researcher physically copying and pasting material. Thus, the researcher is still responsible for interpreting the data, but the physical work is carried out by the software (Bryman, 2012). The software is used in a supporting capacity, rather than as a substitute for the researcher: “they [CAQDAS] will not do anything that you couldn’t do by hand with cards, lists and bits of paper” (Pickford, 2013: 279).

4.10 Limitations and alternative methods

Whilst readability testing is a widely used method of testing written materials in areas such as the health sciences and forensics, they do not cover all aspects of good writing. Presentation style and how the document is deployed are both important aspects of written material that readability scoring fails to acknowledge. As well as this, it should also be noted that readability testing takes a mathematical approach to analysing difficulty. A short but difficult word or a long but generally recognised word will not be picked up by such testing. Despite this, readability tests are widely used, noted as being reliable, and they analyse the

properties of written materials that can help to promote or hamper understanding of a text. The four tests chosen were found to be the most popular and robust tests when the researcher was carrying out the initial investigation into readability testing.

There will always be a degree of interpretation regarding qualitative data analysis, which is shaped in part by the researcher's own motivations, interests, and experience. In order to be self-reflective, the researcher has taken care to ensure the themes chosen have been backed up by the literature review.

The thoughts of those who use the library regarding the AUP has not been recorded for this study. The focus of this research was on the documents themselves, rather than the views of those who use the library's ICT facilities. It can also be difficult to gain insight into what respondents actually think (Gomm 2004; McNeill and Chapman, 2005). Also, it cannot be guaranteed that the same person is answering the whole questionnaire, or that there is no input from other persons (Bryman, 2012). Also, Bryman (2012) notes the possibility of social desirability bias with interviews. Although questionnaires are better than personal interviews in trying to avoid this (Bradburn et al., 1982), there is still a possibility of this influencing respondent answers. The researcher wished to investigate the text and the intentions behind the words used and documents can be very revealing as to how an organisation conducts itself, and the attitudes within (McNeill and Chapman, 2005). By analysing the policies themselves, it was thought key insights into the culture of surveillance and the promotion and restriction of information access would be gained. Policies also have the benefit of being already available, and not produced for the benefit of the study, thus there is no influence from the researcher (Bryman, 2012). It should also be noted, that although the policies give insight into the library service's culture, what happens in practice may be quite different. What has been written in the AUPs is a representation of how the library services wishes to conduct itself, and this might not always be consistently practiced in the actual public library building. This was also important however, for the policy would reveal how the organisation wishes to conduct itself, whether it does or not, which gives key insights into motivations and

the culture behind the policy; whether surveillance is put into practice on a regular basis or not, if the AUP focuses on surveillance this reveals something about the culture of the library service.

Using FOI requests to obtain information regarding the construction of the library AUPs rests on the interpretation of the individual who is charged with dealing with the information request. Whilst efforts were made to make the request as clear as possible, including running a pilot of the question, as demonstrated by the findings a small number of those who answered asked for further clarification.

Although the researcher obtained 99.5% of public library AUPs in the UK, what has been found in this study is UK-specific and therefore cannot be generalised. It would be interesting to investigate the AUPs used by public libraries in other countries. Also, how the results here compare to policies in other areas such as educational institutions.

Although the model AUP compiled by the researcher from the results of this study has used recommendations in place by Sturges and other best practice as indicated by the literature review, and has subjected the policy to readability testing and amended the policy according to the results given, it should be noted that the model policy has not been piloted. The model policy is an intellectual rather than a practical exercise and it is intended that it will be made available, by public dissemination through conference and by using a Creative Commons licence for distribution.

4.11 Conclusion

To reiterate, the research questions posed following the literature review were:

- RQ1 In what ways does the public library AUP document reflect the panoptic principle?
- RQ2 How does the public library AUP encourage and discourage access to information and freedom of expression through surveillance, filtering, and commitment to ethical principles?

- RQ3 How effectively does the AUP balance the care and control elements of public access?

This research used a mixed methods approach to answer the research questions. The research used AUP documents to examine how the public library promotes and prohibits freedom of expression and privacy, and if the surveillance used exhibits aspects of the panoptic principle, as well as finding out how the public library balances the care and control aspects of public access. Firstly, Internet searching was employed to find AUPs from public libraries in the UK. FOI requests were used to obtain the remaining AUP documents, as well as information on who was responsible for formulating the AUPs. Readability testing was carried out on the AUPs obtained, using online readability software and four readability formulas found to be reliable in the literature: the Flesch Reading Ease; the Smog Grade; the Gunning Fog Index; and the Coleman-Liau Index. After this, qualitative content analysis was used to study the text of the AUPs, using the CAQDAS software, NVivo. The following chapters detail the results and discussion of the study.

5 Quantitative results and discussion

5.1 Introduction

In the previous chapter, the methods of analysis for this study were presented. This chapter will present the findings and interpretation of the quantitative methods used, along with a discussion of the results.

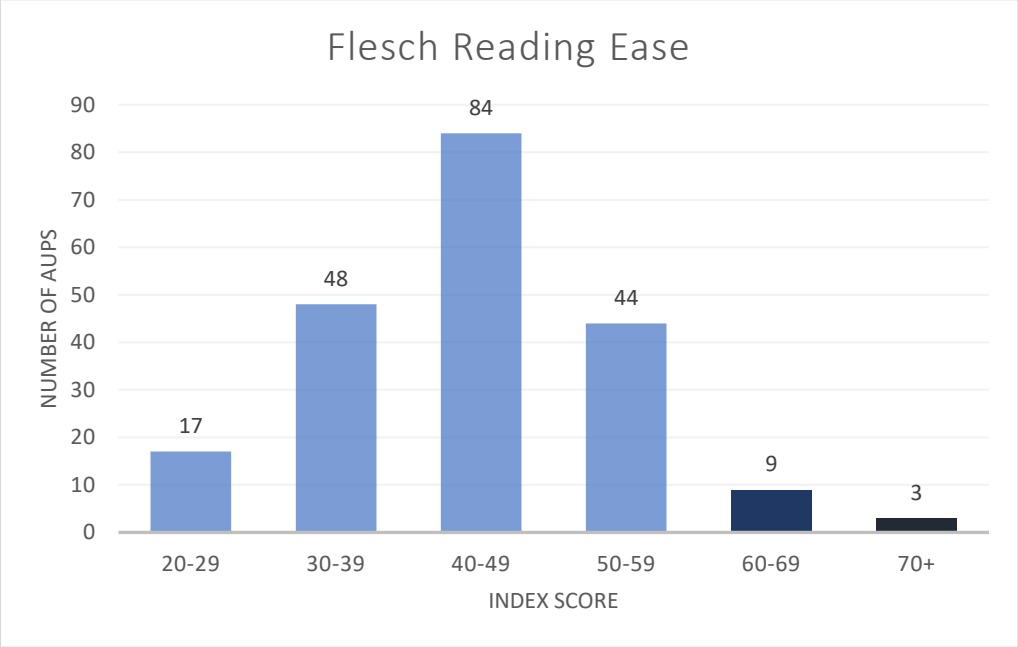
To reiterate, the methods used were the following:

- Data collection was carried out using FOI requests
- Readability testing was carried out across the 205 AUPs collected. The four readability tests used were the Flesch Reading Ease; the Gunning Fog Index; the Coleman-Liau Index; and the SMOG Grade
- Qualitative content analysis

5.2 Readability

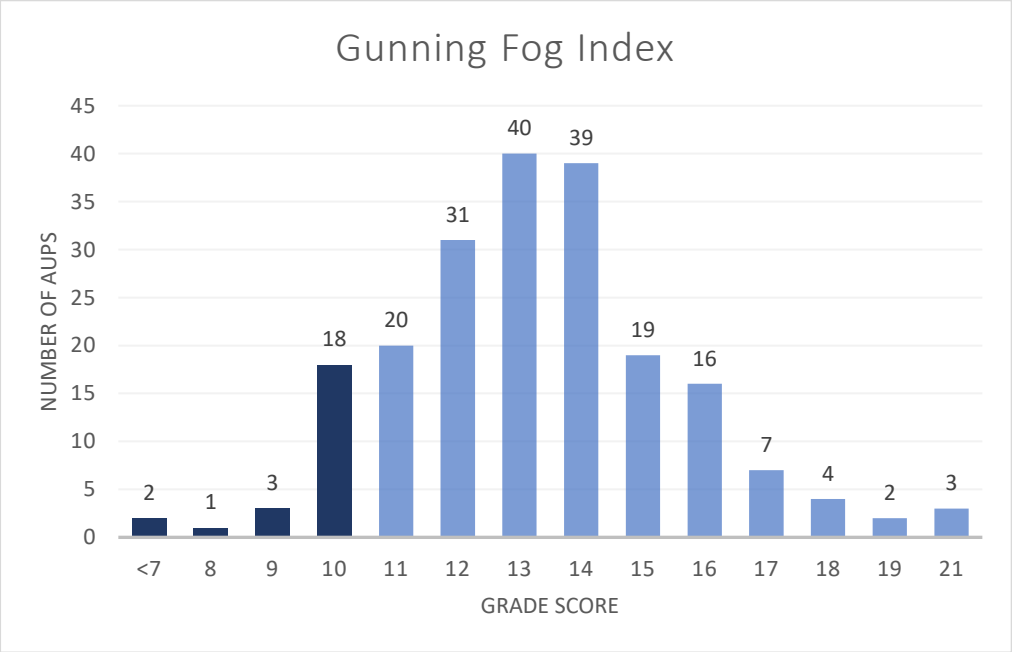
As discussed in the previous chapter, readability is an important aspect of writing text, and contributes to the understanding the reader will have in their comprehension of a piece of text. The AUPs were put through four readability tests: the Flesch Reading Ease; the Gunning Fog Index; the Coleman-Liau Index; and the SMOG Grade. These were chosen for their wide usage and perceived utility as found in the literature: these four tests are seen as reliable and good indicators as to the difficulty levels of a piece of text, and their use is recommended by institutions such as the National Literacy Trust.

Figure 2 Flesch Reading Ease



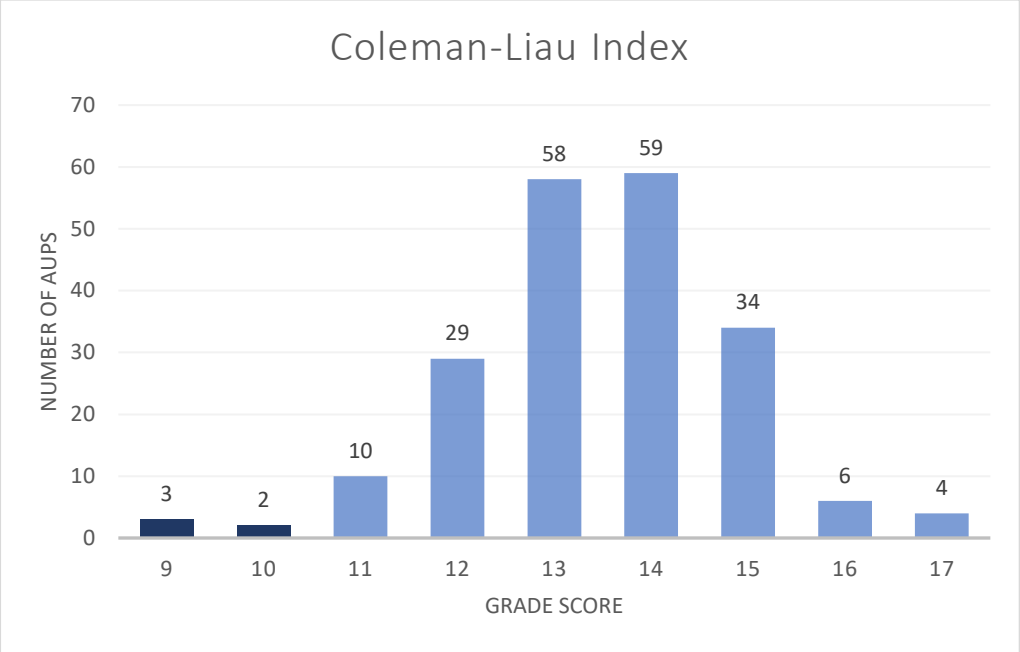
The average Flesch Reading Ease score was 44, rated as difficult. The largest block of AUPs (84 AUPs, 40.9%) fell within the 40-49 mark, with 65 AUPs (31.7%) scoring 39 or less, which is at the very difficult range. Only 12 (5.8%) of the AUPs scored 60+, which is considered standard reading level. The mode for FRE was 33.

Figure 3 Gunning Fog Index



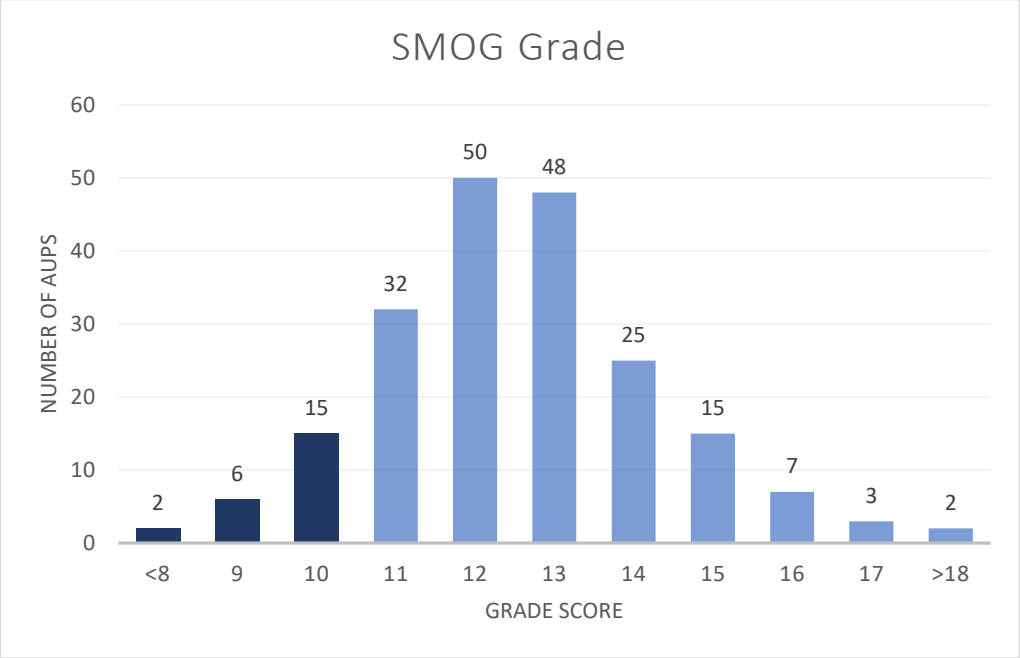
The average Gunning Fog Index score was 13.6, well above the level recommended by Grewal et al. of 7-8 (2012: 1463). Using the National Literacy Trust's recommended score of 10 for US Grade tests, 24 AUPs (11.7%) were of that score or below. The highest Gunning Fog score was 21. Only 6 AUPs (2.9%) scored 9 or less. 130 of the AUPs scored above 12 (63.4%), which indicates a reading level requiring tertiary education. The mode for Gunning-Fog was 14.4.

Figure 4 Coleman-Liau Index



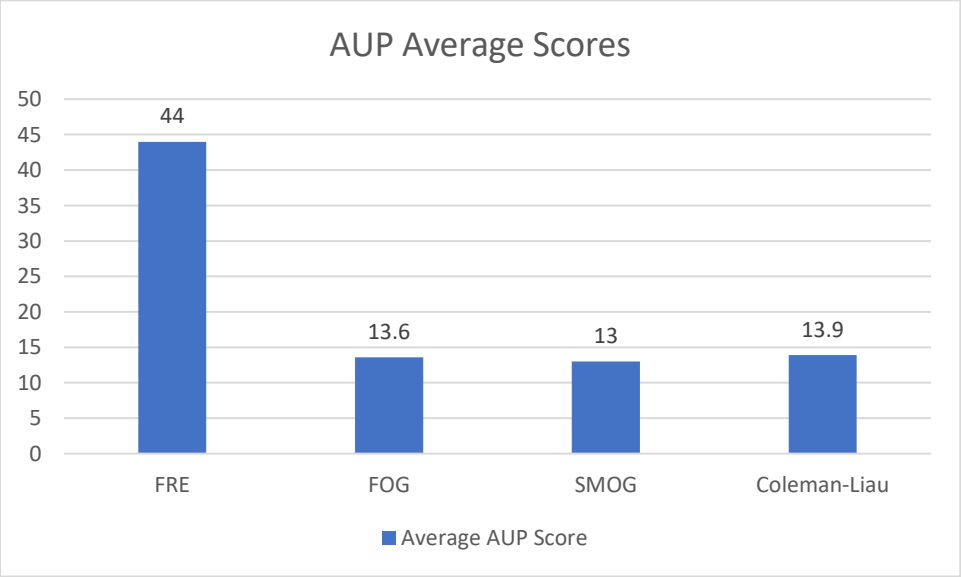
The average Coleman-Liau score was 13.9, at the higher difficulty level – suggesting reading levels requiring further education. 161 of the AUPs (78.5%) scored at 13 or above, with four AUPs scoring 17. Only 5 AUPs (2.4%) scored 10 or below, the National Literacy Trust recommended score. The mode for Coleman-Liau was 15.

Figure 5 SMOG Grade



The average SMOG score was 13, above the National Literacy Trust's recommended reading score of 10. Again, results were varied – 105 AUPs (51.2%) scored 12 or below, and 100 (48.7%) scored 13 or above. Only 22 of the AUPs (11%) scored 10 (National Literacy Trust recommended level) or below. The mode for SMOG was 12.2.

Figure 6 AUP averages



5.2.1 Length

The average word count was 817.5, with 107 being the lowest number of words and 3,797 being the highest. The median count was 650, and the mode 527. The standard deviation was 572.4, making the document closer to 4,000 words an outlier (indeed, this AUP had a long appendix detailing filtered websites categories). It should be noted that it is recommended that documents like AUPs should be short and to the point, however it can also be helpful to provide additional information that may be of use – the AUP in question's bulk of data was an appendix featuring filtered website categories which could potentially be useful for information users.

5.2.2 Readability discussion

The results suggest that the AUPs for public libraries in the UK are not easily readable for library patrons. The variability between documents also highlights a lack of cohesion between one PLA and the next. Overall the majority of AUPs tended to score at difficult reading levels across all four tests, with a considerable level of variability within each test. In all four of the readability categories – the Gunning Fog Index, the SMOG Grade, the Coleman-Liau Index, and Flesch Reading Ease – the AUPs scored at a high level of difficulty, and in some instances were considerably higher than the other documents tested, such as the BBC News website article, which is also designed for a mass audience. This high score reflects other studies that have found a lack of clarity regarding some features of public library AUPs such as filtering (McMenemy 2008; Spacey et al., 2014), and the variable and often lacking content of AUPs generally (Stewart, 2000; Doherty et al., 2011).

As a contract between the library service and the user, it is paramount that this document is written in a clear and understandable way, to make sure patrons understand the terms of access to the computing facilities and not expose the library service to any unnecessary risk (Gaunt, 1998; Höne and Eloff, 2002; McMenemy, 2014). With comprehension hampered, the library patron is less likely to understand the consequences if they were to misuse the facilities, putting both themselves and the library service at risk. As well as the risk of possible misuse, having a difficult readability level can also hamper the patron's awareness

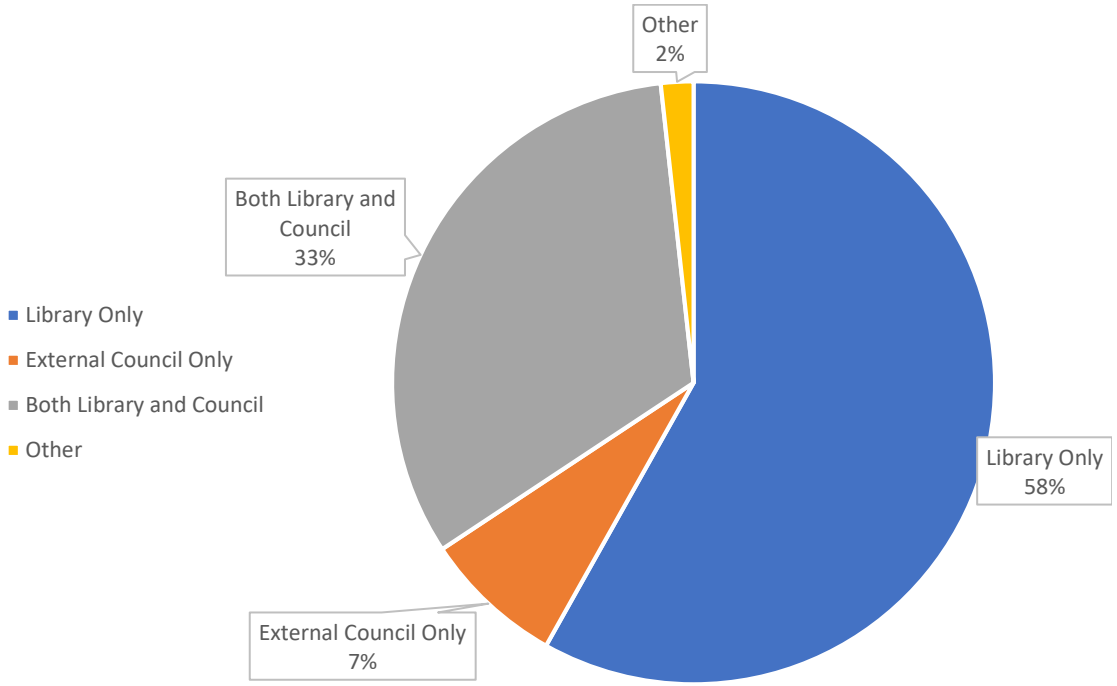
of how the library service can be beneficial to them (McMenemy, 2014). An AUP document that is not easily comprehended for patrons does a disservice.

5.3 Authorship

Along with readability testing, FOI requests were sent out to ascertain the departments of each PLA that were responsible for composing the AUP. This was done both in conjunction with the requests for the documents themselves or on their own if the document had already been located.

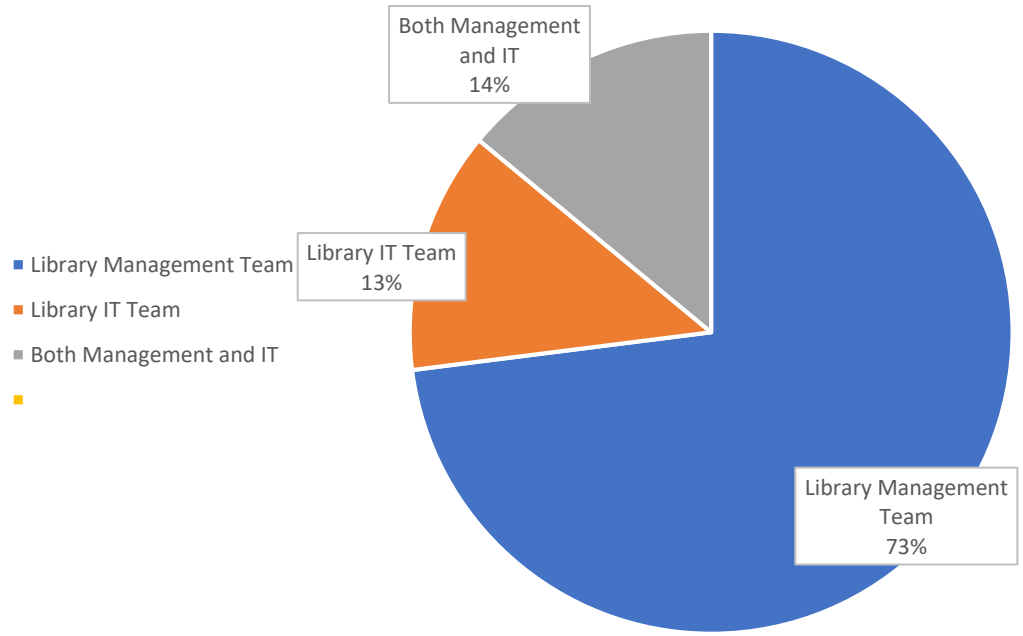
Of the 206 PLAs, 172 provided information on who was responsible for creating the AUP. Of the 34 others 16 did not reply or only gave part of the FOI request by providing the AUP document only. 17 PLAs did not hold the information asked for, sometimes this was further clarified by stating the information is no longer held on file due to the length of time that had passed since its creation. One PLA stated that the information was exempt due to the Data Protection Act. The information provided by the 172 PLAs that did have the information can be broken down into various groups:

Figure 7 Authorship of the AUP – Overall



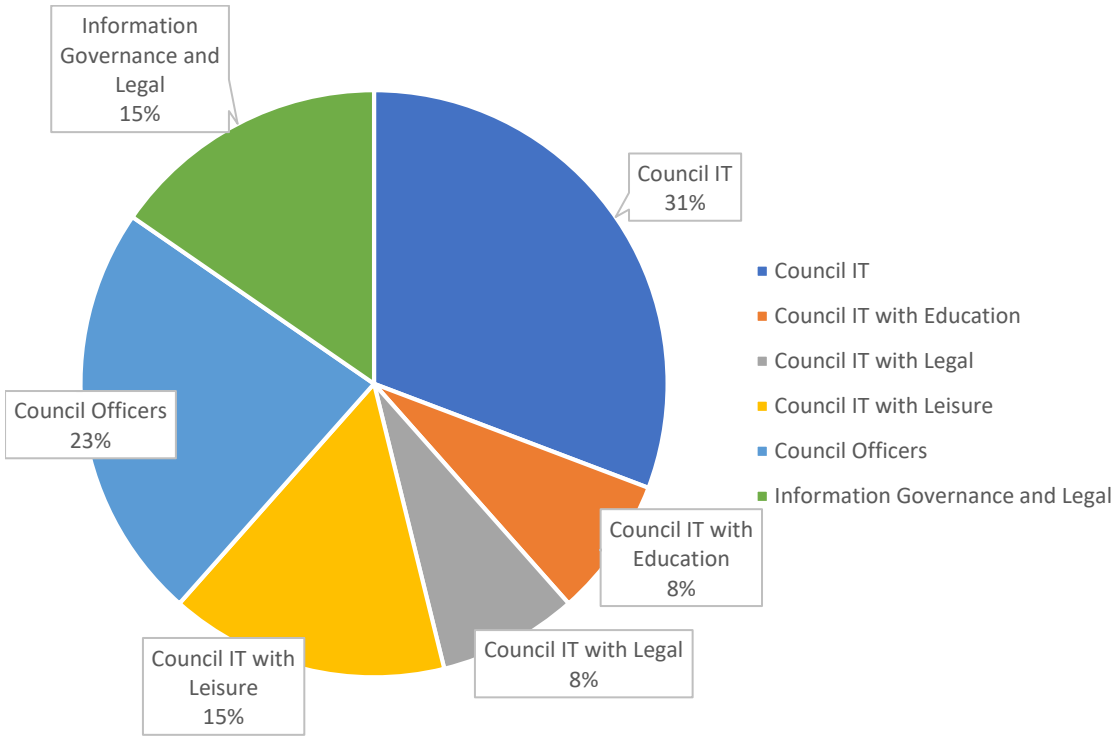
Of the **Library Only** segment, this can be further broken down:

Figure 8 Authorship of the AUP – Library staff only



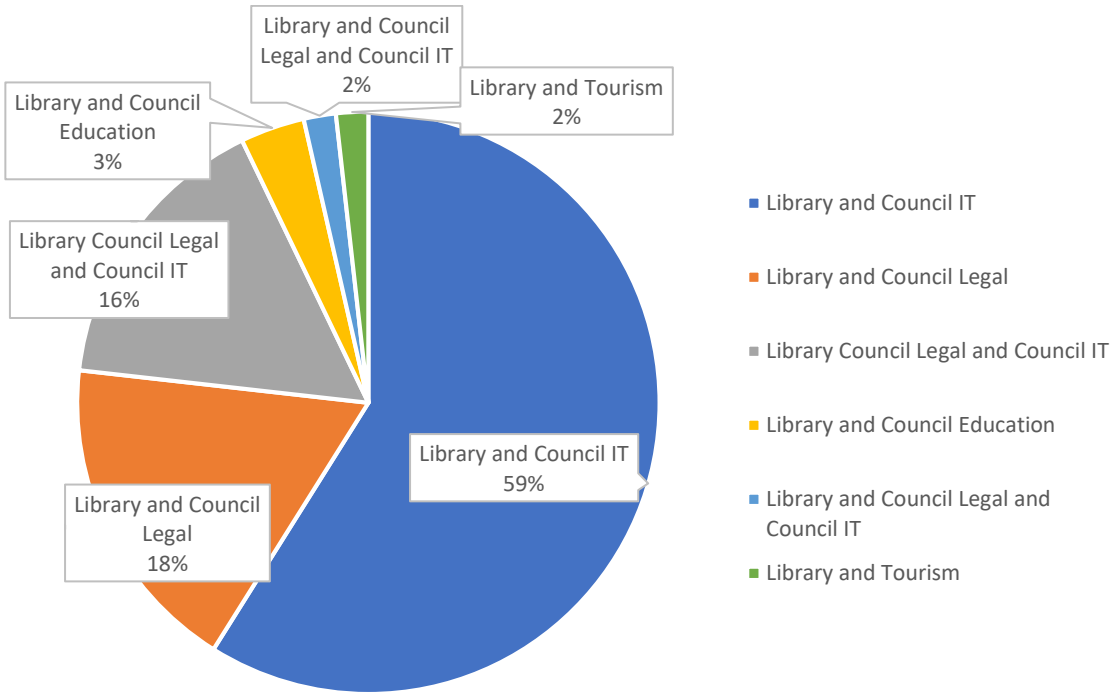
Of the **External Council Only** segment:

Figure 9 Authorship of the AUP – External council only



Of the **Both Library and External Council** Segment

Figure 10 Authorship of the AUP – Library and external council members



When the nodes featuring in the AUPs was compared to the authorship information, it was found that AUPs written by the library service only represented Sturges' elements of an AUP the most: 90% of those written by the library service only had Sturges' elements of an AUP, compared to 84% if the authorship was mixed or 69% if the authorship was council only. Panoptic elements were most represented by council only written AUPs: 92% of council only written AUPs heavily featured panopticism nodes, compared to 87 in mixed authorship AUPs and 76% if the AUP was written by the library service only. Filtering, its efficacy, and how to unblock websites was best represented in library service only written AUPs. Information on unblocking numbers were low – only 18% of mixed authorship AUPs had information on unblocking, with library service only authorship the highest at 37%. CILIP's ethical principles

were best represented by mixed authorship AUPs. A full breakdown appears in the table below, numbers shown are percentages of the number of documents:

Table 5 Authorship element breakdown

AUP ELEMENTS	LIBRARY ONLY	LIBRARY & COUNCIL	COUNCIL ONLY
CILIP PRINCIPLES	61%	66%	53%
FILTERING	81%	78%	8%
EFFICACY OF FILTERING	57%	55%	54%
UNBLOCKING	37%	18%	23%
NOT WATCHING	1%	3%	0%
MONITORING CARE	14%	20%	15%
MONITORING NEUTRAL	26%	39%	23%
PANOPTICISM	76%	87%	92%
STURGES	90%	84%	69%

External council and library staff were represented most well in cities. AUPs written by library staff only were mostly represented in rural areas. The AUPs written by external staff only had no significant numbers in rural or urban areas but instead were mixed. Interestingly, there was no real significant geographic distribution in terms of country. The different groups of author were widely varied. The various disparate parties employed to help compose the AUPs perhaps suggest that a single AUP for all PLAs, written by a mixed group of experts, including those from the library itself, legal, IT, and other council representatives, would serve the libraries and their patrons better. A single AUP would require less overall manpower, and could be rigorously edited to ensure legal compliance and also readability.

The next chapter details the results and discussion of the qualitative content analysis.

6 Qualitative results and discussion

As discussed in the methods chapter, this research used qualitative content analysis to analyse the AUPs. Qualitative content analysis allows for an interpretative method of analysis than quantitative, allowing for both the manifest and latent meanings to be analysed (Mayring, 2000; Figgou and Pavloupolos, 2015). The themes used for analysis were informed by the literature review. Although the results were quite varied, some themes were shared by AUPs geographically similar or close to one another.

6.1 Panopticism and Lyon

As mentioned in the literature review, surveillance has become an integral part of modern society (Haggerty and Ericson, 2000; Groombridge, 2002; Lyon, 2002; Monahan, 2011), being an important part of how modern institutions function (Giddens, 1990; Gallagher, 2010). It seems that in the public library it is no different. Similar to findings by Willson and Oulton (2009), the MAIPLE project (Spacey et al., 2014), and Gallagher et al. (2015), monitoring, both electronic and physical, was mentioned in a majority of the AUPs. Although it is important to ensure crime and inappropriate usage is not being carried out in the public library, care should be taken to make sure any monitoring that is being carried out is framed in such a way as to reassure patrons that the surveillance is necessary, legitimate, and appropriate to prevent crime and protect the library and its users. Critical aspects of the panoptic principle, such as controlling surveillance, discipline, and compliance all featured in the AUPs. Surveillance carried out in the public libraries included both overt and covert monitoring, using both physical and electronic means of doing so. Whilst surveillance may be seen as a necessity in the public library, as both a deterrent to any would-be criminals and for evidence in the case of any crimes taking place, as well as to protect the users of the library service, the way it has been conveyed by some of the AUPs is perhaps heavy-handed and overly authoritarian in tone, with surveillance described in a such a way as to appear as a method of regulation, rather than one of protection. Monitoring was varied amongst the AUPs, but those that specified monitoring was not in use, tended to be clustered geographically.

6.1.1 Monitoring control

Information was coded as monitoring control if the surveillance being carried out was specifically for regulatory or disciplinary purposes. The monitoring control node was referenced in 119 of the AUPs, with 143 references overall.

Monitoring was stated to be in use so staff could check if patrons were misusing the system or facilities:

- “We reserve the right to check on usage to ensure that this Policy is adhered to.” (AUP 112)
- “Use of the Internet will be monitored to ensure that it is not being used improperly.” (AUP 147)
- “The Council can, and will, monitor access to internet sites, and access to any material in breach of these terms may be subject to further action. We reserve the right to check your internet usage without informing you.” (AUP 180)

Sometimes this was context-dependent, as in:

- “Staff are permitted to view computer screens at any time during a session. Any individual found engaged in any inappropriate activity as defined above will have their access withdrawn and in the case of illegal activity, will be reported to the appropriate authority.” (AUP 1)
- “All usage will be monitored, and anyone found infringing the Public Computer Use Agreement will be stopped from using the service.” (AUP 47)

Monitoring was also used to ensure library users were using facilities for what the library deemed as appropriate use:

- “Accounts of all users will be monitored through the use of a software programme to restrict access to prohibited material and to monitor inappropriate usage of free time for job searches.” (AUP 200)

Prior to this, AUP 200 states that:

- “All users are expected to demonstrate a responsible approach to the use of resources made available to them” (AUP 200)

AUP 200’s use of monitoring is to check users are using facilities for the correct purpose – the monitoring is not carried out for safety reasons, surveillance is being used for checking up on user behaviour and is thus a controlling rather than caring use of surveillance. This seems a particularly heavy-handed use of monitoring. The mention of a software programme, omniscient in its observance of users, as a means of checking up on what the user is doing while using the ICT facilities suggests an electronic panopticon. Everyone is under observation to ensure that they behave. By mentioning that all users are subject to this monitoring, also suggests the surveillant assemblage (Haggerty and Ericson, 2000); everyone is under the web of surveillance, no-one is outside, because it is controlled by a machine.

As well as prevention of misuse, monitoring could also be used after the fact, when misuse had already occurred or after a report had been made:

- “Please remember that each computer keeps a record of how you have used it. These records may be accessed in the event of any allegation of misuse.” (AUP 12)
- “[NAME REMOVED] reserves the right to inspect log files and computer files if misuse is reported by a member of the public or library staff.” (AUP 31)

Although surveillance can be used in this way to ensure illegal or inappropriate activities are not being carried out in the public library setting, sometimes the use of monitoring seemed to serve the purpose of ensuring patrons were browsing material that the library deemed as acceptable, and at times seemed invasive. As with other aspects of the AUPs, there was a tension in the documents between preventing misuse and providing a safe service through routines such as surveillance, whilst allowing users to feel comfortable to browse the Internet and access information freely. This tension is echoed by previous studies such as Randall and Newell’s investigation into public library use of

video surveillance, in which librarians felt both that surveillance is an invasion of privacy, but also necessary for keeping individuals safe, and a practice that many patrons did not seem to mind (Randall and Newell, 2014), and Sturges' survey of users in institutions of higher education which found 75% of users to be acceptive of monitoring (Sturges et al., 2003).

6.1.2 Monitoring care

Text was coded as monitoring care if the surveillance being carried out is for reasons of care such as protection and safeguarding of information users. 35 AUPs were coded under this node, with 40 references overall.

Some monitoring was used directly for the safeguarding of the patrons using the facilities:

- "To ensure the safety of our customers we monitor use of the Internet, including web sites visited." (AUP 170)
- "For your protection, and that of all users, Internet use is monitored and filtered." (AUP 191)
- "In order to ensure a safe enjoyable experience for all of our members, we operate a robust monitoring and filtering practice at all times. This practice operates both electronically and manually." (AUP 192)

Monitoring was also used to help support the library service:

- "[NAME REMOVED] Council reserves the right to monitor and log all types of computer activity, including web sites visited, in order to plan better services" (AUP 56)
- "Monitoring of computer systems and networks is necessary to maintain optimum performance of the service." (AUP 55)

This sort of monitoring, used in order to plan for a more efficient, tailored service has been promoted in some sectors of the library sector (Estabrook, 1996), however, it should be used with caution – patrons should not be used as data subjects in the same way that a business

or a corporation might. Using patron data to provide an optimum service could potentially be a beneficial idea for both the public library and the patron – providing the library with the ability to keep up with modern trends and remain ahead of potential competition, and giving the patron a more efficient, tailored service. Unlike a corporation however, the public library is not there to make a profit for its investors. There is a transactional nature of the surveillance used by corporations, with consumers gaining rewards from data mining, such as ease of use (Marx, 2006), with the surveillance part of the overall consumer experience (Zurawski, 2011). There is a conflict when information is used in this way in the public library. The public library is provided for the benefit of all its users, and is a mostly free establishment. Monitoring for better services should be used with caution. As Sturges et al. (2003) found from users, privacy concerns tended to be low with regard to libraries, however, this is partly due to the fact that patrons trust that the library staff will handle their data with care. Straying too far into the realm of loyalty cards and data-gathering turns the public library into a business-like institution, instead of a cultural service, with information on patrons changing into something resembling a product (Sturges et al., 2003). Transparency and clarity for the user is key. What sort of monitoring is this? Is it simply monitoring online traffic to ensure an optimum online service? Or is the library using patron data to tweak aspects of the service? Most AUPs simply stated that monitoring was being used to "plan better services and to ensure you keep to this policy." An insight into how this monitoring is being used would provide the user with a clearer picture of how their data is being used, along with a better connection to the library and what it does.

A number of the AUPs highlighted that the library was a shared space and so monitoring was necessary:

- "All websites which are accessed by users are logged. This also applies to users of laptops and other devices… Of particular concern is the accidental access by children of obscene or other inappropriate material." (AUP 160)

- “Our responsibility We will take measures to protect children accessing the internet. This may include the use of filters and staff supervision.” (AUP 117)

Surveillance can be used to both promote and discourage freedom of expression and information access. If used in an encouraging way, to protect patrons, surveillance can help visitors feel safe and can promote exploration. Surveillance is perhaps seen as a warranted and wanted safety barrier; something that is appreciated, even if it is not necessarily effective (Gill and Spriggs, 2005). Visitors to the library can be safe knowing that staff are watching over them, and their computer sessions are filtered to ensure that there is no access to potentially upsetting images and text. It should, however, be used with caution. If surveillance is being expressed in such a way as if to control patrons, it can be stifling. The library service must balance concerns about privacy alongside the necessary steps the service must take to ensure Internet access is safe for both the institution and the patron themselves (Marco, 1993). There is a question about where the line for surveillance should be drawn in regards to protecting users. It is far too easy to stray into overuse and dependence on surveillance.

6.1.3 Monitoring neutral

Monitoring was sometimes mentioned by the AUPs, but not in such a way as to be for controlling or caring reasons. For example:

- “Library staff will monitor your use of the internet and other computer software, remotely or by visual checks.” (AUP 39)
- “All access to the internet is monitored and recorded by [NAME REMOVED].” (AUP 63)

There is no discernible reasoning behind the monitoring, simply that it is taking place. Monitoring neutral was a rarer node than monitoring control, but more common than monitoring care, with 64 references in 61 different sources. Privacy commitments are important to the information profession – the ethical principles of CILIP highlights both the promotion of human rights, of which privacy is one, and also a concern for both

confidentiality and privacy when dealing with information users. The intrusion into a user's privacy when using certain types of technology comes into direct conflict with these ethical principles (Zimmers, 2010). Thus, surveillance must be used with caution. A user that knows they are being monitored may be less likely to search for websites that discuss sexual health or other similarly private matters, and this effectively stifles freedom of expression and access to information (Skaggs, 2003), another crucial part of CILIP's ethical principles and a key part of general autonomy and selfhood (Fried, 1992; Barendt, 2007). The use of surveillance must be used cautiously and the patron must be informed of the reasons for doing so – by not giving any explanation here, the library service is crossing over into privacy intrusion, without adequate justification.

6.1.4 The panoptic gaze

140 of the AUPs contained the panoptic gaze node, with 167 references to this theme overall. Some AUPs had very explicit instances of the panoptic gaze. There were a number of statements regarding the potentiality of surveillance, leaving the patron somewhat in the dark as to whether surveillance is actually taking place. Likewise, the use of checks, and the unknown quality to the surveillance are key parts of the panoptic machine. This uncertainty is a key part of panopticism; the "apparent omnipresence" (Bentham and Bowring, 1843) is a core part of the Panopticon's function:

- "[NAME REMOVED] Council respects users privacy whilst using the Internet, but users should be aware that Internet access is monitored and that random checks will be made on the sites visited. The Library keeps a record of every Web page accessed." (AUP 22)
- "You must not use the internet and email for deliberately searching, sending or receiving any material which is illegal, obscene, offensive, abusive or intolerant, or in breach of confidence, copyright, privacy or any other rights. Routine checks are carried out to ensure the internet is used appropriately." (AUP 154)

- "[NAME REMOVED] reserves the right to monitor Internet use and that staff are permitted to view computer screens at any time. Information on my specific internet usage may be released to authorised enforcement agencies where required by law under specific exemptions of the Data Protection Act." (AUP 106)

The notion of random or routine checks exhibits the panoptic principle: the user will not know at any one time of they are being watched or not, thus will constantly be vaguely aware of someone possibly watching them. AUP 106 mentions that staff are permitted to view computer screens at any time – again, this notion of the unverifiable watcher, who could watch at any time, also indicates panopticism.

AUP 71 in particular evokes panopticism through the usage of messages being posted to users:

- "Staff can… Monitor live usage of public access computers and can post messages to users if unsuitable material is accessed." (AUP 71)

Whilst it could be suggested the use of an on-screen message is more discreet than a member of staff confronting the user, it is hard not to think of the electronic Panopticon through the use of constant monitoring and messages popping up on-screen to deter users from wrongdoing. The idea of an unseen watcher is emphasised by random messages popping up on the user's screen. Monitoring is developed further by the AUP:

- "Websites accessed by all users are logged and monitored by [NAME REMOVED] Council." (AUP 71)

AUP 71 has taken care to make sure its users understand that their session is being monitored both in real time and after the fact. These different types of surveillance, both live and recorded for posterity, suggest a web of surveillance that the patron is trapped in, much like the way the inmate is exposed to the guards in the tower of the Panopticon. The prisoners in the Panopticon can see the tower in the centre of the building watching them, and they are keenly aware at all times of its presence. Likewise, being informed that they are

being watched remotely means that although library patrons will be aware their use of the ICT facilities is being monitored, they do not know when this monitoring is being carried out. Although patrons should of course be informed that they are being monitored, the use of random and remote checks could serve to make the patron wary of how they use the facilities, as Foucault describes panoptic surveillance having the effect of being “permanent in its effects” (Foucault, 1991: 201) even if the surveillance is not constant. The extent of surveillance, by Internet logs, filtering, and email monitoring reflects the findings of the MAIPLE project. In particular, the use of live monitoring and messages being posted to user screens reflects the MAIPLE project’s findings, in which access was said to take place in a “virtual Panopticon” (Spacey et al., 2014: iv). The uncertainty of when they are being watched, along with the unverifiable nature of the watcher, are key themes in panopticism. Such surveillance could lead patrons to start self-censoring their behaviour, in a chilling effect. It could also make the patron reticent to use their library for Internet access, if they feel like they are being checked up on, or if messages are flashing up on their screen.

The use of punishment was also made uncertain:

- "The Library and Information Service will monitor usage of the Internet. Any attempt by users to access prohibited sites or to receive or transmit offensive or undesirable material, or otherwise misusing the facilities, may result in action being taken." (AUP 188)
- "Records of which users were using each machine at any particular time will be maintained for six months. This information may be provided to law enforcement agencies for the purpose of prevention or detection of criminal activity." (AUP 140)
- “Details from the automatic booking system are kept for the purpose of analysis. This information may also be provided to law enforcement agencies for the purpose of prevention of criminal activity.” (AUP 128)

The AUPs use the word “may” in regards to action being taken by the library service so the patron is left feeling uncertain, which is key to panopticism. AUP 128 adds a further area of

uncertainty stating that details are kept from the automatic booking system for “the purpose of analysis”. This analysis could simply be routine quality checking, however by being so vague the library user has no real idea as to what sort of analysis this is. The mention of law enforcement agencies straight after this may make the user feel like the analysis is being used to monitor their behaviour to decide if the activities they are carrying out online are cause for concern.

AUP 27 explicitly states that a user’s privacy will not be guaranteed:

- “[NAME REMOVED] operates a web / e-mail filtering and monitoring policy in accordance with our legal obligations. You should therefore not use the computers to download or access information which is personal to you, or private or confidential, as we cannot guarantee your privacy.” (AUP 27)

Privacy is one of the public library’s key principles, and its importance is noted by various ethical guidelines and practitioners (e.g. Sturges et al., 2001; ALA, 2008b; CILIP, 2013; McMenemy et al., 2014; Harper and Oltmann, 2017). For a patron to be able to explore information freely, they need to be able to feel like they have a sense of privacy (Campbell and Cowan, 2016). For an AUP to specifically state that privacy will not be guaranteed is troubling. Although the library service must be upfront about any potential privacy violations, the service user must also have confidence in being able to access information unhindered. Such statements potentially discourage access, and could lead to patrons self-censoring their Internet behaviour.

6.1.5 General monitoring observations

Surveillance is carried out both physically by library staff, and electronically through the monitoring of e-mail and browsing habits:

- “[NAME REMOVED] reserves the right to inspect log files and computer files if misuse is reported by a member of the public or library staff.” (AUP 31)

- “[NAME REMOVED] can monitor access to Internet sites through both manual and electronic systems. This will also allow [NAME REMOVED] staff to check that a user is not committing a criminal offence relating to the use of the internet.” (AUP 51)

Some AUPs detailed their use of monitoring in a very explicit and transparent way:

- “Such monitoring may include, but is not limited to:
  direct observation of computer screens
  observation using CCTV (where applicable), images from which may be recorded
  examination of audit trails of activity which has taken place.
  Information obtained as a result of monitoring may be provided to law enforcement agencies for the purpose of prevention or detection of criminal activity. Information recorded using CCTV will be processed in accordance with [NAME REMOVED] policy on CCTV usage.” (AUP 128)

AUP 128 is being transparent here, by being upfront that monitoring will be taken in various forms. However, as the “is not limited to” phrase suggests, it by no means details all the types of monitoring that the library uses.

Monitoring is carried out both covertly and overtly, via both physical and electronic means. Sometimes the execution of monitoring was not confirmed, just suggested as a possibility:

- “Although we do not routinely monitor use of the system, activity is logged and can be investigated should the need arise.” (AUP 152)
- “You should be aware that council security systems are capable of recording all transactions, website visits and emails made on library computers. Any public access of illegal, offensive or controversial material may be subject to further action.” (AUP 91)

Both of these AUPs note that the service has the capability of monitoring, although the library service does not do this actively. This potentiality of surveillance evokes the panoptic principle. Whether it is being used in actuality or not, the patron is aware of the possibility.

Note here that it is the council, rather than specifically the library staff themselves, that are said to be monitoring. This is mentioned by other AUPs also:

- “In order to prevent misuse, library staff (or other employees of [NAME REMOVED] Council) may monitor the activity taking place on any computer provided for public use.” (AUP 128)

The fact that these other employees are not specified may be of concern to the patron. Who exactly is monitoring their computer use?

Similarly, AUP 70 states that:

- "You will be prevented from any further use of public access computers if you access any site which, in the opinion of council officers, including library staff, is considered to be illegal, threatening, obscene, racist, pornographic or likely to be of concern to the police or other regulatory organisation" (AUP 70)

Instead of noting library staff or other employees of the council, AUP 70 states council officers first, then includes library staff after this. Whilst in a traditional library setting, any misuse of facilities or complaints by patrons would be dealt with by library staff, it is interesting that AUP 70 puts general council officers first, then follows with library staff, when traditionally, library staff would take precedence (or perhaps sole decision-making) for deciding what is considered to be of concern.

AUP 144 notes that others outside the council may also monitor patron usage:

- “We can and will monitor access to internet sites and users should also be aware that use of the internet may also be monitored and recorded by third parties such as internet service providers and individual websites.” (AUP 144)

When discussing children’s usage, a number of AUPs notes that the library is not responsible for what they access: monitoring is something that is provided by the caregiver.

AUP 18 states that:

- “Parents/Guardians of children and young people are responsible for monitoring material accessed by them.” (AUP 18)

Some AUPs made sure to stress that although monitoring was being carried out, user privacy was still very important to the library service:

- “The Council recognises an individual’s general right of privacy but reserves the right to monitor where a complaint alleging a breach of the policy is received.” (AUP 110)
- “6.6. The Council does not use the public computers to store any data relating to citizens.

  6.7. The Council reserves the right to monitor and log all types of activity across the service.

  Activity includes access to e-mail and web sites.

  Monitoring may be performed both electronically and manually.

  The Council will however endeavour to respect users’ right to privacy at all times.” (AUP 60)

These AUPs make sure the patron knows that privacy is important, and monitoring will only be used in certain circumstances, or in such a way that makes sure to respect the user. This can help to reassure patrons that monitoring is being carried out in a controlled and necessary way and can help to address possible privacy concerns users may have due to the use of monitoring. This was not a consistent sentiment across the AUPs however. The library service has to make sure that the public library is a safe space for the community to use, and part of this is ensuring that the facilities are not used to disturb others or commit criminal activities. However, the link between surveillance and discipline was frequently mentioned together in the AUPs, rather than as a method of keeping individuals safe. Using surveillance to regulate behaviour can have a stifling effect on freedom of expression, as the patrons may feel as if their privacy is being invaded; surveillance has been noted to have a sterilising effect in urban areas (Koskela, 2002). The use of surveillance methods such as filtering can have a chilling effect on patrons (Kline, 1999), where they may feel like they

cannot express themselves fully due to possible repercussions if they search for the wrong thing (Schauer, 1978). Privacy is important for self-development and autonomy (Moore, 2003; Cohen, 2013), and it is an integral part of freedom of access and expression; a user needs to feel like they have the freedom to look for information as they wish when using the library (Gorman, 2015). As a public institution and a shared space however, the library also has a duty to the public good and the community it serves.

If public libraries are to use surveillance, especially remote methods of monitoring, they should properly inform the patron of such activities, in a clear and concise, yet fully informed way. The library service must take care how it describes its use of surveillance to the patron. Surveillance can help to maintain the library as being a safe place for patrons, but there are problems with its potential overuse. The line over which the watchers may cross can be ambiguous; it could prove easy to justify heightening surveillance, and it can be dangerous if this is left unchecked. In the public library, surveillance should be used with a strong justification for why it is being carried out. Some of the AUPs did state that types of surveillance such as checking user logs would only be used in certain circumstances, however these were sometimes described in a threatening way, as if to control user behaviour.

Whilst highlighting that user privacy will be respected, AUP 104 makes sure to differentiate between different types of users:

- “Library and other staff monitoring the use of equipment will respect the privacy of legitimate users at all times.” (AUP 104)

This statement echoes both Foucault’s ideas regarding the dichotomy facilitated by institutions (such as good/bad, mad/sane) and also Lyon’s notion of “social sorting”, which is a key aspect of modern controlling surveillance. Users are separated into categories of those that are legitimate and those that are not.

A number of AUPs cited the Data Protection Act, noting that monitoring would be carried out in compliance with the Act. AUP 101 for example, underlines the library service's commitment to Data Protection and preserving public trust with respect to how their data is handled by the service:

- "[NAME REMOVED] ensures that all employees and volunteers follow Data Protection guidelines. [NAME REMOVED] Libraries recognise that it is only through continued public confidence in the upholding of Data Protection principles that confidence in the library itself can be maintained which is vital to the library's role in the community and the community's right to know." (AUP 101)

68 sources mention Data Protection or the Data Protection Act. 44 AUPs mention the Data Protection Act in relation to patron data and how the library service will store or use patron data. Of the remaining 24, 22 AUPs mentioned the Data Protection Act in relation to patron usage of the facilities, usually alongside other legislation such as the Computer Misuse Act or the European Copyright Directive. One of these AUPs specifically stated monitoring was carried out by the library to ensure patrons themselves were complying with legislation such as the Data Protection Act. The remaining two AUPs had the Data Protection Act in a detailed appendix of different legislation that pertains to IT usage.

AUP 61 notes under its "Filtering and monitoring policy" heading that:

- "Staff may monitor your use of the Internet at any time." (AUP 61)

It is perhaps a concern that the library service's monitoring policy is simply "we monitor". There is no real justification here. There no explicit reason for monitoring users, just that it takes place.

AUP 51 gives a detailed explanation regarding the library service's use of monitoring:

- "[NAME REMOVED] can monitor access to Internet sites through both manual and electronic systems. This will also allow [NAME REMOVED] staff to check that a user

is not committing a criminal offence relating to the use of the internet. Records of Internet access are retained for up to 12 months. Any public access of illegal material shall be the subject of further action. Offensive or controversial material may also be the subject of further action. If in any doubt about the nature of the material being accessed, guidance should be sought from a member of staff." (AUP 51)

The AUP tells the user why monitoring is used in a clear and transparent way and outlines exactly what happens to their data. The AUP also explains what the user should do if they are unsure about any websites they access.

6.1.6 Care and control

As well as caring and controlling surveillance, text was coded for general references to the idea of care and control. All of the AUPs contained references that were caring or controlling in nature, some overt, and some covert.

6.1.7 Care

98 of the sources featured the general care node, with 318 references overall.

Care was expressed as protection for users:

- "Please take care if:

  Anyone you meet on the internet asks for any of your personal details (such as address, or your telephone number, your picture, or your credit card or bank details)
  Anyone asks, through an e-mail or social media arrangement, to meet you, either through online contact or in person." (AUP 5)
- "The following policy has been developed in order to safeguard both users and their interests." (AUP 1)
- "[NAME REMOVED] Council cannot be held responsible for the privacy or security of your activities and urges caution when undertaking financial transactions online." (AUP 4)

16 AUPs included a statement in the introduction explaining that the policy was created to safeguard the service and the community and users it serves**.** Although the statement from AUP 4 is in large part a disclaimer to ensure patrons understand that user activities are their own responsibility, it also demonstrates care for the patron by warning them to be careful when they exchange money over the Internet.

Care was also expressed as helping users to have a good experience at the library:

- "To help you get the best out of the Internet, [NAME REMOVED] Council has developed this Acceptable Use Policy (AUP)." (AUP 2)
- "To ensure fair and safe access to ICT, and to facilitate homework support, each library will reserve one or more PCs for the exclusive use of children and young people." (AUP 86)

These are clear indicators of caring for the citizens who are going to be using the service. AUP 2 states that the reason the policy was created is to help patrons have a fulfilling time online. In AUP 86 the library service wants to facilitate children's access to the computers. Enabling others is one of the criteria that Lyon identifies as caring for individuals in his description of caring and controlling surveillance. Care for children and facilitating their access was an important aspect of the library service for a number of the AUPs:

- "In [NAME REMOVED] we have a responsibility to ensure that the infrastructure and technology provide a safe and secure environment for children and young people." (AUP 182)

Some AUPs emphasised the communal and reciprocal nature of the library:

- "Please Help Us to Help You" (AUP 12)
- "Respect other persons using the library." (AUP 28)

Both of these statements exhibit care – AUP 12 explicitly notes it wants to help patrons. AUP 28 attempts to foster a respectful environment in the library.

AUP 82 has this statement which ends the document:

- “**Questions, comments and concerns**

  [NAME REMOVED] wants to know what you think of its Internet service. Please feel free to ask questions or raise concerns at any time. If your concern cannot be resolved immediately by a staff member, please complete a comments form so that the matter can be raised with a senior manager.” (AUP 82)

AUP 82 ensures the patron that the service is approachable, and statements such as this one are a good way of building relationships between library services and their users. Instead of ending the document with a disclaimer, or information regarding disciplinary action, like many of the AUPs, AUP 82 ends on a positive note.

6.1.8 Control

Control was coded in 118 of the sources, with 241 references overall.

- “You must read and accept the following terms and conditions before you can use this computer. Please keep to them - if you don't you may not be allowed access in the future.” (AUP 33)
- “The Library reserves the right to take appropriate action to ensure compliance with the policy, including withdrawing the right to access the Internet.” (AUP 40)
- "Obey the requests of the library staff." (AUP 28)
- “You must read and accept the following terms and conditions before you can use this computer. Failure to comply with this policy will result in members having their Library Learning Centre membership suspended.” (AUP 4)

Words like “obey” and “failure” have strong negative overtones. AUP 33 uses particularly threatening language to make sure users stick to the conditions of the AUP. Outlining the consequences of behaviour that is disruptive to the library service is an important part of the AUP, however it can be done in such a way as to not sound overly threatening. This use of language is similar to the findings by Gallagher et al., who noted the “authoritative and

condescending" (Gallagher et al., 2015: 586-587) language in their study of 32 AUPs from Scottish PLAs.

Sometimes control was emphasised through conditions set out for the patron:

- "Individuals who are granted the right to use the public Internet services are permitted to do so, on the following conditions:… If you do not comply with the above conditions we may evict you from the library and/ or withdraw your right to use the Internet in [NAME REMOVED] Libraries and the police may be contacted." (AUP 12)

AUP 12 sets out conditions for the patron and makes sure they adhere to them by outlining sanctions if they do not comply with said conditions. These statements clearly aim to regulate the patron's behaviour and are thus controlling in nature.

AUP 94 states that access for patrons will be withdrawn for a variety of reasons:

- - "[NAME REMOVED] reserves the right to stop anyone using the computers at any time but particularly where there is access of illegal, offensive or controversial material."
  - "[NAME REMOVED] prohibit specific online activities that we consider to be illegal, offensive, obscene, abusive or troublesome to others."
  - "Access may be withdrawn if: [NAME REMOVED] considers your use of the computers to be undesirable or not in the public interest." (AUP 94)

Words and phrases such as "not in the public interest", "controversial", and "undesirable" could be too opaque for the user to fully understand what sort of websites or materials the AUP is referring to. The AUP does note that activities that may be troublesome to others will be prohibited, but this is nestled alongside more controlling language, such as the phrase "[NAME REMOVED] reserves the right to stop anyone using the computers at any time" which is quite authoritarian.

Similarly, AUP 7 states that:

- “Users must not deliberately visit, view, or download any material from any website containing pornographic, abusive, racist, violent or illegal material or material which is offensive in any way whatsoever. The Council’s decision as to which websites fall into these categories is final.” (AUP 7)

Both of these AUPs make it clear to the patron that they are the arbiters of decision-making. Phrases and terms that are vague allow for a wide variety of materials to fall into the net of what is unacceptable. The threat of sanctions and the stated authority of the library service or council indicate that these statements are controlling in nature.

6.1.9 Both care and control

A lot of the AUP content strived to find a balance between protection, freedom of expression, and privacy:

- “[NAME REMOVED] does not prohibit specific on-line activities as long as they are not considered to be illegal, offensive, obscene, abusive or troublesome to other computer users.

  Internet users should not access, download, transmit or print any obscene, offensive or illegal material. Staff reserve the right to terminate any Internet connection, which, in their opinion, does not meet this requirement.” (AUP 51)
- “7) When visiting chat rooms or newsgroups you must not use language that may cause offence, and you must disconnect if such language is used by other chat room participants. Be careful when giving personal contact information in a chat room.” (AUP 99)

These statements have aspects of both care and control. AUP 51 is controlling in that the statement is trying to regulate patron behaviour, but in such a way that it emphasises that the patron should be able to browse as freely as possible. AUP 99 uses authoritative language – “you must not” – whilst also giving protective advice and information to the patron.

6.1.10 Compliance

A large part of the panoptic principle is the concept of discipline, and regulation. A focus on compliance, as well as misuse and sanctions for misuse, were also indicators of panopticism in the AUPs. Compliance was the most heavily featured node: it was featured in 204 sources, with 752 references to compliance altogether. The word ‘comply’ and its stems (“compliance”, “complying”) were used in 85 sources, with 140 references overall. Other words such as “abide” were also used frequently; “abide” featured in 73 sources, with 96 references overall. “Obey” was also used in one document. Only one AUP had no references to compliance – this particular source did not ask for any guidelines to be observed, or mentioned acceptable or unacceptable usage parameters, rather the AUP was simply a list of what the library and IT service provided.

Compliance was framed in a number of ways. AUPs varied by tone, striking educational, authoritarian, or communal notes. Some AUPs referenced other users and emphasised mutual respect and sharing of the facilities:

- “For the Internet to operate in a manner that satisfies the majority of its users, all users need to observe some rules and behaviours governing their use of it.” (AUP 2)
- “I will respect the privacy and sensibilities of other library users, and I will not cause noise, or display text that may be reasonably viewed as obscene or offensive.” (AUP 3)

Although AUP 2 makes sure to refer to the shared aspect of the library service, the use of the word “rules” strikes an authoritarian tone.

Some AUPs placed the emphasis on the user, and was written as if from their perspective, using phrases such as “I agree that I will” or “I am fully responsible for.” Writing in such a way can help the patron to feel more involved with the contents of the AUP. Other AUPs were written in a detached manner, listing the terms under headings such as “misuses” or “agreements that the user makes”:

- "Computer users are required to respect the library byelaws" (AUP 9)

Others spoke directly to the user:

- "**You <u>must</u>:…**

  and you must <u>NEVER</u>:…" (AUP 5)

Whilst speaking directly to the user, the use of the bold and underline both stresses the importance of the points being made, and also emphasises the rigid, almost demanding nature of the statements**.** A number of the AUPs used strong phrases such as "users must" or "you must not" to compel patrons to follow the AUP. The word "must" appeared 767 times altogether across 182 of the AUPs. This spanned a number of different aspects of the AUPs, observing important legislation, disclaimers, respecting other users, and following the AUP itself:

- "**You must:** comply with the relevant laws" (AUP 2)
- "Users participate in these activities at their own risk and must indemnify the Council against any claim or demand that may be made against them as a result of their activities." (AUP 7)
- "When using these facilities, you must abide by the following conditions of use" (AUP 205)
- "Users must respect the privacy of others and must not transmit information, photographs or images of another individual without that individual's knowledge and consent" (AUP 132)

Compliance was often used as a way to threaten users into maintaining good behaviour:

- "Failure to abide by these standards may result in the loss of Internet, computer, and Library privileges." (AUP 165)
- "The use of the network is a privilege not a right, and may be taken away if abused." (AUP 80)

- “You must read and accept the following terms and conditions before you can use this computer. Failure to comply with this policy will result in members having their Library Learning Centre membership suspended.” (AUP 4)

It was also interesting that users were being threatened with privileges being taken away in response to what the library perceived as bad behaviour. 23 of the AUPs made a reference to computer or library privileges.

Compliance was often paired with monitoring:

- “We may monitor your use of the computer / mobile device, including web sites visited, in order to plan better services and to ensure you keep to this policy.” (AUP 3)

This exact phrase was shared by six of the AUPs.

Compliance appeared in the introduction to AUPs, in conjunction with sections detailing usage parameters, and in the patron declaration sections of the AUP. AUPs often had lists of agreements that the user had to make in order to use the facilities, sometimes in the form of a declaration.

6.1.11 Discipline

Power and discipline are key aspects of Foucault’s theories on panopticism, with the Panopticon itself being the pinnacle in self-regulating, disciplinary power. The AUPs contained various references to power display and panoptic discipline. Surveillance of patrons was often mentioned in conjunction with disciplinary measures if the patron is caught engaging in unacceptable use of the facilities. Power was illustrated through council authority and the threats of “further action” by the council if the patron persists in unacceptable behaviour. This echoes Gallagher et al.’s study of AUPs in Scotland, where prescriptive language was used to exert authority (Gallagher et al., 2015).

196 of the AUPs make a reference to sanctioning individuals for misuse, with 186 referring to some form of ban. Of the remaining nine AUPs, five make reference to misuse or criminal

offences but do not mention any sort of disciplinary procedure, three AUPs have no information on disciplinary procedures, and one AUP does make reference to users being responsible for any damage or negligence in regards to PCs, and also mentions staff being able to terminate their session at any time, but these were not in conjunction with one another. Another AUP notes that:

- "We may monitor your use of the computer / mobile device, including web sites visited, in order to plan better services and to ensure you keep to this policy." (AUP 3)

AUP 3 however, does not mention any consequences of misuse, or indeed how exactly they ensure users keep to the policy. Perhaps it pertains to filtering, however this is not made clear, and this lack of information alongside the use of monitoring makes it difficult to discern if the library service has disciplinary procedures or not.

Some AUPs detail sanctions against the user, including stages such as a verbal warning, suspension, and then termination. Five AUPs make reference to a verbal warning. 36 AUPs mention a user's session being terminated because of misuse. Some AUPs also note that the library service may inform other libraries in the area if a patron misuses the facilities (e.g. where the library authority is part of a consortium).

- "Library & Customer Services will not deny legitimate access to information by any member of the public, but recognises that access to electronic resources may be open to misuse and abuse. This policy has been produced in order to protect the interests of the Service and the community it serves. Failure to comply with the AUP's terms and conditions may result in the use of the IT facilities being suspended, withdrawn; or may lead to prosecution." (AUP 145)

This AUP does a good job of highlighting why the AUP is place, why the patron should comply with its conditions (to protect the community) alongside consequences of misuse. Highlighting reasons about why a patron should not misuse the facilities such as for

protection of the library service or its community is a positive way of applying the AUP and possible sanctions. Alongside words such as prosecution and failure, the AUP mentions legitimate access and the community.

- “As well as the loss of computer privileges, other disciplinary options may be applied by the Council, including criminal prosecution.” (AUP 120)

Using vague wording such as “other disciplinary options” is perhaps unnecessary and overly negative.

The phrase ‘failure to comply’ was used by 21 of the AUPs. Whilst it is necessary to make users aware of any possible outcomes of misusing the facilities, using phrases such as “failure to comply” are heavily negative. The use of such language does not encourage access to information for users. This is similar to Gallagher et al. (2015), in that the explicit phrasing could be perceived as threatening for some users. The use of such language goes to reinforce the authority that the public library has over the user. As an institution that should promote access to learning and freedom of expression it is a concern that a number of the AUPs use such negative, authoritarian language.

Two quotes, very different in tone, from the same AUP:

- "The Council can and will monitor access to internet sites, and access to any material in breach of these terms may be subject to further action. We reserve the right to check your internet usage logs without informing you." (AUP 145)
- "Library & Customer Services staff have the right to instruct computer users to remove unsuitable images or text from the screen if, in the staff member’s judgment, the image or text is displayed in such a way that other library users cannot reasonably avoid viewing it. Please remain sensitive to the fact that you are working in a public environment shared by people of all ages." (AUP 145)

The first quote is concise, but very blunt, with the threat of the unseen watcher. The second quote presents power display and discipline but in such a way as to appear non-threatening,

and gives detailed reasons as to why such disciplinary action would occur. By linking potential disciplinary action with protection for other members of the library, it both justifies the reasoning for such actions and gives the patron a good, perhaps more concrete reason not to do certain actions.

- "You are bound by the Libraries Terms & Conditions and should adhere to them. We will not tolerate any offensive, racist, pornographic or illegal material brought into the library. If caught you will be subject to the Libraries disciplinary procedures and the police will be notified. You will also be banned for a period of time, which will be decided at the libraries discretion." (AUP 128)

Presumably the banning period will depend upon the seriousness of the transgression. It would perhaps be helpful to be given more concrete information here, however.

Like compliance, discipline was often closely tied to monitoring user activities:

- “The library service will monitor use of the internet, any attempt by users to access prohibited sites or other unauthorised material may result in further action being taken.” (AUP 174)

6.1.12 Display of power

Display of power was a frequently referenced node, appearing in 187 of the AUPs, with 439 references overall.

Sometimes it appeared as a consequence to misuse:

- “I understand and accept that if I do not abide by these conditions [NAME REMOVED] Council will withdraw my access to the Internet in [NAME REMOVED] Libraries, and may take further action as appropriate.” (AUP 114)
- “If you breach the above policy we may terminate your internet session without notice and suspend your access to the facility.” (AUP 201)

These were coded as display of power because the library or council is the arbiter of whether the patron has access to the Internet or not, and also the vague terms in which the statements are made; what is the "further action" as defined by AUP 114? This is a somewhat threatening phrase that could potentially put a user at unease. The idea of being able to terminate a session without notice is also a strong display of power.

Displays of power were reflected in word usage, tone, and phrasing:

- "Staff have the authority to terminate any internet connection that contravenes this policy, and to prohibit the offender from future use of the service." (AUP 5)
- "Users must not deliberately visit, view, or download any material from any website containing pornographic, abusive, racist, violent or illegal material or material which is offensive in any way whatsoever. The Council's decision as to which websites fall into these categories is final." (AUP 7)
- "Anyone that does not abide by these conditions will have their access to the People's Network computers in [NAME REMOVED] Libraries withdrawn and the council may take further action as appropriate." (AUP 9)

AUP 5's use of the word "terminate" along with "authority" and "prohibit" clearly marks the staff of the library as having power over the patron. AUP 7 states that the local council's decision is final, which is authoritative. AUP 9 notes that the council may take further action, showing clearly that the council is the one that makes the decision, and has the authority to take further action, or not.

This passage from AUP 165 strikes different tones – the first paragraph is authoritative, and also negative in tone, this is then followed with a more positive paragraph emphasising respect for others and outlining guiding principles rather than rules:

- "All electronic traffic originating from the [NAME REMOVED] Public Library connection shall be in accordance with these Acceptable Use Standards. Failure to

abide by these standards may result in the loss of Internet, computer, and Library privileges.

Acceptable Use

Use of the Library's computers shall be guided by the following principles: Respect for the privacy of others." (AUP 165)

Sometimes it manifested in subtle statements of gatekeeping, as in:

- "In order to gain access to the Internet via this [NAME REMOVED] Council terminal you must agree to the following:" (AUP 114)

The use of "gain access" highlights that it is the council that has the authority here.

6.1.13 Banning and sanctions

186 of the AUPs made reference to the banning node, with 292 references overall.

Some AUPs referred to sessions being terminated or "further action being taken".

- "The Library and Information Service will monitor usage of the Internet. Any attempt by users to access prohibited sites or to receive or transmit offensive or undesirable material, or otherwise misusing the facilities, may result in action being taken." (AUP 146)

Discussions surrounding banning were often coupled with references to the police or legal authorities:

- "Any individual found engaged in any inappropriate activity as defined above will have their access withdrawn and in the case of illegal activity, will be reported to the appropriate authority." (AUP 1)
- "Anyone that does not abide by these conditions will have their access to the People's Network computers in [NAME REMOVED] Libraries withdrawn and the council may take further action as appropriate." (AUP 9)

- “Any such use will result in you being denied access to the computers in any [NAME REMOVED] Library and may result in prosecution.” (AUP 19)

Two AUPs used the word evict:

- “If you do not comply with the above conditions we may evict you from the library and/ or withdraw your right to use the Internet in [NAME REMOVED] Libraries and the police may be contacted.” (AUP 12)
- “In cases of criminal or disruptive behaviour customers may be evicted/ excluded from Library premises and have their membership suspended. The Police will be informed if illegal activity is suspected.” (AUP 68)

The use of the word evict is particularly interesting. It is both formal and authoritarian. It is not just banning a patron, it is ejecting or expelling them, as if a tenant from a rented property, or a pupil from school (this is further reinforced through the use of “excluded”).

Users could be simply suspended for a designated period of time or given an outright ban. Sometimes other stages were included, like verbal warnings.

- “You are bound by the Libraries Terms & Conditions and should adhere to them. We will not tolerate any offensive, racist, pornographic or illegal material brought into the library. If caught you will be subject to the Libraries disciplinary procedures and the police will be notified. You will also be banned for a period of time, which will be decided at the libraries discretion.” (AUP 128)

The stages were not consistent nor consistently mentioned across AUPs:

- “I understand that if I break any of the listed conditions regarding computer internet use, I may be banned for up to 3 years from using any computer facilities at any libraries within the [NAME REMOVED]” (AUP 185)
- “Failure to comply with these standards will result in library staff terminating your session. You may be temporarily or permanently banned from using the computers.

Suspected illegal acts will be referred to the Police for investigation and may lead to prosecution." (AUP 67)

- "Failure to adhere to this policy may lead to withdrawal of services either on a temporary or permanent basis." (AUP 110)
- "Any User who breaches the Acceptable Usage Policy three times will be permanently banned from using Public ICT Resources on their third offence. The first and second offences will be subject to four week suspensions for each occurrence as detailed above. The third offence will result in access being withdrawn on a permanent basis. Written confirmation of this will be issued." (AUP 84)

Nine of the AUPs mentioned an appeals system being in place:

- Five AUPs gave full details on submitted an appeal, including how to submit an appeal and the process of reviewing the appeal
- Three AUPs stated appeals could be submitted, details of which could be given on request
- One AUP stated appeals could be made but gave no further information

Discipline and power is further reinforced when there is no mention of how to appeal against sanction decisions, and when the AUP states that staff have absolute discretion. 186 AUPs mention banning, but only nine give details on how to appeal the decision made.

6.2 Sturges' essential features

6.2.1 Aims and objectives

Of the 205 AUPs, 60 had information on the library service's aims and objectives, usually in the form of an opening statement, or as part of the overall introduction, for example:

- "[NAME REMOVED] County Council's Libraries & Archives service provides public access to the Internet as part of its role as a supplier of information and in support of lifelong learning. This access is offered to people of all ages as an enhancement of their existing entitlement to library services." (AUP 88)

This forms part of AUP 88's opening statement, alongside a request that those under 16 gain permission from their guardian, and a note about the library's license for streaming live television.

Some of the AUPs featuring aims and objectives were close geographically, and had very similar opening statements, suggesting the AUPs might have been based on one another. Given the importance of this feature of the AUP, in defining what the library service hopes to offer its users, and to help the user to understand the rest of the AUP, it is not very helpful that 145 of the 205 AUPs do not outline their aims and objectives. It may not be apparent what exactly a particular service is going to offer – the ICT facilities may be reserved for recreational or educational use only. Service is not uniform and what one library service permits another may bar so outlining the aims and objectives of the library service should be paramount and a staple of every AUP. It is helpful to outline what the library service is aiming for to give the patrons a better, fuller, understanding of the service they are being provided.

AUP 171 has a clear opening preamble:

- "Summary

  This explains how internet access in libraries and record offices is provided and monitored, how people who do not have [NAME REMOVED] library cards can access the internet, what expectations we have of web users, what happens when someone misuses the internet access, and how they can appeal if they do not agree with what has happened." (AUP 171)

This opening explains why the AUP is there and provides a concise rundown of its contents. Although it is hoped every user will read the AUP, not all of them will, and by providing a summary at least those less likely to read the whole document will perhaps jump to a section they find to be of importance.

AUP 180 has this opening:

- “We are delighted to provide access to computers and the internet to our computer users. They provide access to a wide range of resources and opportunities for information, education and entertainment. We do, however, recognise that access to electronic resources may be open to misuse and abuse. This policy has been produced in order to protect the interests of the library service and the community it serves.” (AUP 180)

The AUP has a positive opening with some indication as to what the facilities are to be used for. The AUP also provides information on its purpose and notes the misuse that can take place using IT facilities, and what the service does to care for its users. By stating the reasons as to why the policy has been produced, the reader may have a better idea of what the policy is about, and thus more of a reason to read it.

AUP 91 has a detailed opening preamble and includes its vision after the introduction:

- “**Vision**

  The Service aims to utilise ICT facilities / resources effectively to ensure that both the needs of the customer are met and that these resources are used to contribute to other areas of development within the Service.” (AUP 91)

AUP 32 starts with no real introduction. Instead it launches straight into what the user agrees to do or not do – there is no statement of welcome, vision, or aim for the service:

- When users sign onto our system they agree that: ·

  I will take due care of the Council computer equipment that I use to access the Internet.

  I will not take any deliberate action to interfere with the proper operation of the systems… (AUP 32)

63 of the AUPs provided no opening preamble but instead launched straight into the terms and conditions of using the service. Of the 142 AUPs that did feature an opening statement:

- 41 stated the purpose of the policy
- 64 stated that the AUP is an agreement
- 57 described the role of the library
- 88 mentioned what the library service offers to its users
- 87 had a formal statement introducing the policy and its application
- 17 had information on membership
- 6 mentioned surveillance or monitoring
- 33 mentioned that the policy is there to safeguard patrons or protect them
- 20 stated the user's responsibilities

The opening section of the AUP varied, sometimes by a drastic degree. Some AUPs provided a detailed introduction, with the vision for the service and what it offers, along with details on membership and eligibility for use. Others had one sentence. Some had nothing at all.

6.2.2 Eligibility

Of the 205 AUPs, 81 featured information regarding eligibility. Eligibility parameters need to be laid out in terms of whether the service is open to all, or just members, and what sort of access should be expected for children. Of the 81 AUPs that referenced eligibility, 57 were coded as describing eligibility fully. That is, not all of the AUPs discussed who is eligible to use the library facilities in a full way. For example, some AUPs gave information regarding use of the facilities by children, but not about whether access is restricted to members only, or if the service can be used by visitors outside the authority. Some AUPs simply stated access was "open to all", whilst others gave more detailed information:

- "**Who can use library computers?**

  1. Any member of the library. You will need your library card number and PIN.

  2. Visitors to the area can have access by providing proof of name and I.D.

  3. Adults and Young Adults are not permitted to use Children's PCs." (AUP 31)

- “To log on to a computer a membership number and PIN is required. A PIN can be requested from a member of library staff who will require confirmation of membership details e.g. confirmation of date of birth/address/phone number etc.
  Non members can log on using a visitor number and PIN provided by library staff.” (AUP 9)

Whilst it may be presumed that those visiting the library from outside the area will ask staff for information regarding eligibility for using the IT facilities, it is still important to include this information in the AUP, so that those reading the AUP online before they visit the library will have this information, or those patrons who are members but may not be aware of the parameters for access can check the details.

AUP 22 begins with this statement:

- “You may use this PC provided that you meet all legal requirements and do not cause disturbance or offence to other users of the library.” (AUP 22)

The first part of the statement is rather vague – which legal requirements is the AUP referring to? The second part, whilst clearer, is not exactly an encouraging way to start an AUP. It gives attention to the library community and the shared space of the facilities, but does so in quite a strong, negative way.

6.2.3 Scope

The information on the scope of the service varied greatly. Some AUPs were written in such a way as to suggest an assumption had been made by the writers that those using the facilities would know what sort of facilities the library provided. However, it is clear that some library authorities allow for much more restricted personal use than others, so the AUP should never assume the patron has information which they do not. Some AUPs opted to discuss points such as inappropriate use, what to do if equipment does not function correctly, and other safety guidelines. Scope covered a range of access parameters such as USB use, filtering policy, and printing costs. Some delineated printing costs, separating into

categories of black and white, or colour, whilst others simply stated at the end of the document that all printing costs that had been incurred must be paid for by the patron. Sometimes information was scarce, with only minor references to the use of filtering, informing patrons about the lack of television licensing in the library, or passing references to printing without a breakdown of the costs involved. Some AUPs reserved information on the scope of the service only for information regarding bandwidth restrictions on heavy usage such as gaming websites.

Some AUPs gave detailed information such as:

- "[NAME REMOVED] Library Service provides computers for public use in all libraries as part of its role to cater for the educational, recreational, information and cultural needs of individuals.
  [NAME REMOVED] Library Service provides its members with:
  Access to the World Wide Web
  Access to mail services such as Hot Mail
  Scanning facilities
  Printing facilities in both black and white and colour (charges apply)
  Use of Microsoft Office and Publisher." (AUP 140)

AUP 91 opens with a description of the library service and the facilities that patrons may use:

- "Within [NAME REMOVED] Library Service there are [NAME REMOVED], all of which have access to a wide range of ICT facilities via the Community Information Network. This infrastructure has enabled the Service to provide free access to the Internet, email, office facilities, information sources, both accredited and non-accredited courses, and the library CD ROM network." (AUP 91)

When coding for information that fell into the Scope node uses such as accessing chat rooms were sometimes listed under "prohibited uses" rather than that the library does not offer such facilities. Whilst it may be indeed, prohibited, it is interesting that some AUPs

chose to categorise it in this way, rather than simply stating chat room facilities are unavailable. Some AUPs gave advice including not to give personal details out on Internet chat rooms. Whilst helpful, it would perhaps be informative to note that personal use such as Internet chat rooms are available in that particular library service. Other AUPs mentioned chat rooms, but in a peripheral way, such as:

- "7) When visiting chat rooms or newsgroups you must not use language that may cause offence, and you must disconnect if such language is used by other chat room participants. Be careful when giving personal contact information in a chat room." (AUP 99)

Prior to this, the AUP made no mention as to whether chat room usage is allowed in the library, or indeed gave any such information on personal usage.

- "6. [NAME REMOVED] Libraries reserves the right to refuse further computer access to any individuals accessing or distributing materials which are deemed to be illegal or unacceptable or have the potential to offend or disturb others, particularly abusive forms of marketing, violence or pornography, and materials which could incite hatred or discrimination on the basis of race, religion, gender or sexual preference. Accessing chat rooms is not allowed and [NAME REMOVED] Libraries reserves the right to refuse further computer access to any individuals accessing chat rooms." (AUP 6)

Whilst some chat rooms do exist to discuss and disseminate views that may be racist, sexist, or abusive, chat rooms themselves are simply vehicles for such topics and are neutral unless specifically designed to be outlets for offensive speech. Some AUPs listed chat room websites in their prohibited list which included websites on criminal activity or other offensive websites without any real context. This mischaracterises the basic function of chat rooms and is perhaps unnecessarily authoritarian. AUPs were not consistent on the use of chat rooms as some AUPs actively encouraged the use of chat rooms, or listed chat rooms as a

service the library provides alongside e-mail and scanning facilities. Other AUPs stated that chat rooms were available for use, but recommended caution due to the anonymous nature of such networks.

Similar to chat rooms, the use of library ICT facilities for television was also varied across AUPs. Rather than being framed as something that public libraries do not hold a license for and therefore do not provide, television viewing was listed by some AUPs as a prohibited or forbidden usage, sometimes in the same category as pornography or uploading computer viruses. For example:

- “Live television broadcasts: You may not use library computers to view live television broadcasts (which require a television licence), but you may view non-live (archived) television programmes.” (AUP 46)

With explanation:

- “Under the terms of TV Licensing the viewing TV programmes as they are being shown on TV in the U.K. (i.e. 'live' broadcasts) is prohibited.” (AUP 18)

This appears in its own section, before information about retaining work on USBs, and quite separate from the list of misuses of the IT facilities. This is similar to AUP 39:

- “TV programmes must not be watched as they are broadcast live on People's Network computers. There are no restrictions on 'non-live' programmes such as those available on Channel 4 'On Demand' (4OD) or BBC iPlayer.” (AUP 39)

In another AUP, live television is amongst a list of prohibited uses:

- “Copyrighted material, live TV broadcasts, threatening or obscene material, pornographic material, material protected by trade secret or licence.” (AUP 14)

Similarly to live television, AUP 139 states that financial use is also prohibited:

- “The following actions will not be acceptable and will result in the individual's Internet access being withdrawn:…
  Online financial transactions.” (AUP 139)

It is perhaps problematic that something as innocuous as online financial transactions are being framed in such a way.

Sturges notes that part of setting out the scope of the service includes letting patrons know about any limitations on the service – in particular, whether access to the Internet is filtered or not. Of the 205 AUPs, 36 did not refer to filtering, or were unclear on whether it was used or not. For example:

- “If a user inadvertently accesses material which they believe to be inappropriate, or which distresses or disturbs them, they should immediately turn off the monitor and report the incident to a member of staff, who will take appropriate action.” (AUP 147)

Taking “appropriate action” certainly suggests some sort of filtering mechanism, but it is not clear to the reader if this is definitely the case. Considering the widespread usage of filtering software found by other studies, it seems that some AUPs are omitting important information about the Internet service. Filtering is an important part of access management for public libraries and should be mentioned in the contents of the AUP.

AUP 9 states that:

- “Some file types are blocked in order to minimise the spread of viruses onto our system. These include some executable, compressed, JavaScript, VBscript, audio and video file types.” (AUP 9)

This provides a clear and concise explanation about what sort of files are blocked, and why this is the case. This is then followed with guidelines for those wishing for further information, and that a full list is available on request. This way, the user is not bombarded with a large list of file-types, which may cause confusion if they are not comfortable with using

technology, or may cause them to bypass the paragraph completely if they simply see lists of information. The user is presented with a list of the most popular types of file, along with guidance for those seeking further particulars. This is more informative and less severe than simply stating those watching live television will be subject to prosecution.

Sometimes the scope defined was quite vague:

- "All e-mail must be phrased inoffensively and used for a proper purpose. The following in particular (but not exclusively) are prohibited through e-mail:
  Creating, sending or storing any abusive, offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
  Harassment in any form (including sexual and racial harassment)
  Breach of copyright. Circulating third party works by e-mail is not allowed, unless the author's consent has been obtained in advance." (AUP 151)

AUP 151 has given some detail as to what is prohibited in regards to e-mail content, however the first line states that e-mail must be phrased inoffensively and use for a proper purpose. What sort of speech offends can vary from person to person, what is perhaps more problematic is what constitutes a proper purpose. Is casual e-mail chatting a proper purpose? The AUP goes some way to define what the library service views as a proper purpose by the list of prohibited uses of e-mail that follows, however it notes that this list is not exhaustive.

AUP 200 states that:

- "All users are expected to demonstrate a responsible approach to the use of resources made available to them." (AUP 200)

Further down the document, the AUP notes that users will be monitored:

- “Accounts of all users will be monitored through the use of a software programme to restrict access to prohibited material and to monitor inappropriate usage of free time for job searches.” (AUP 200)

The AUP makes no mention of job searches before or after this statement. Scope is defined in a limited way that is not clear or transparent enough for users.

6.2.4 Illegal use

Almost all of the AUPs mention illegal usage of the ICT facilities. The three that did not contain information regarding illegal usage focussed on the practicalities of the facilities such as booking, printing costs, and children’s use of computers. Illegal use mainly focussed on copyright, with 166 of the AUPs mentioning copyright or copyright legislation. Other legislation included the Computer Misuse Act 1990, referenced in 30 AUPs, the Telecommunications Act 1984, referenced in 15 AUPs, and the Data Protection Act 1998, referenced in 61 AUPs (as well as asking patrons to abide by the Data Protection Act, AUPs also discussed the library’s obligation to this legislation as well). A lot of the AUPs made references to specific laws, in varying levels of detail. The Computer Misuse Act was mentioned by 30 AUPs. Sometimes it was given context as in:

- “You must… Not attempt to bypass security systems to gain unauthorised access to any computer. Any attempt to do so is an offence under the Computer Misuse Act 1990 (c. 18) and the individual may be liable to prosecution.” (AUP 21)
- “Only the named library member may access library PCs or library Wi-Fi. This membership is not transferable to any other person (Digital Economy Act 2010 and Computer Misuse Act 1990).” (AUP 63)
- “It is illegal under the Computer Misuse Act 1990 to attempt to gain access to any computer system, or alter data, where you have not been specifically authorised to do so.” (AUP 161)

Five of the AUPs do this. Three AUPs list the Computer Misuse Act and other relevant legislation such as the Data Protection Act in an appendix with more detailed explanations

as to their content. The rest of the AUPs give no real context as to the legislation, sometimes simply listing Acts:

- “Legislative requirements

  It is a user’s personal responsibility to comply with the following legislation:

  -Data Protection Act 1998

  -Computer Misuse Act 1990

  -Copyright Design and Patents Act 1988

  -Obscene Publications Acts 1959

  -Obscene Publications Act 1964.” (AUP 202)

Whilst it is helpful of the AUP to point out the relevant legislation that the user must follow, it is not necessarily helpful to the user to be presented with a wall of text like this. Also, whilst it is helpful to point to the relevant legislation pertaining to computer usage, from an educational point of view, simply listing off legislation might not be an ideal way to demonstrate proper Internet usage for patrons. A list of legislation with no real context may only serve to muddy understanding, rather than clarify it. Space may be paramount, however a line describing the legislation may suffice, or mentioning the legislation in a more constructive way when describing unacceptable use might be a better way to handle such information. An appendix is also a useful way to deal with complex information that might hamper the flow of the document and the reader’s comprehension of the policy.

One AUP opened with this statement:

- “The ICT facilities in the libraries must be used for lawful purposes only and this use must comply with relevant legislation. If unlawful action is involved users may be placing themselves at risk of prosecution. E-mail and other electronic communications and files are admissible in court as evidence. [NAME REMOVED] Council operates a monitoring system.” (AUP 93)

Whilst part of the AUP should certainly deal with how ICT facilities should be used (i.e. in a lawful way), starting a document with references to prosecution and evidence admissibility does not project a particularly friendly atmosphere. This type of statement could have the potential effect of making the patron less willing to use the library e-mail facilities if they fear what they say may be used against themselves in a court of law.

A number of the AUPs mentioned the local police authority. Indeed, four AUPs opened the policy with the statement that the owners of the premises were working with the local authority to prevent access to unlawful or offensive material over the Internet.

6.2.5 Unacceptable use

Like illegal use, unacceptable use was featured in a majority of the AUPs and was one of the most featured nodes in the study, with 202 of the AUPs featuring the unacceptable use node, with 563 references to this node overall. Misuse would be expected to feature in the AUPs – outlining what constitutes inappropriate behaviour and usage of the facilities is a key part of the AUP, being one of the elemental features as defined by various AUP guidelines (e.g. Scott and Voss, 1994; Palgi, 1996; Sturges, 2002; McMenemy and Burton, 2005; ALA, 2007b; Laughton, 2008), and also as an important part of disclaiming the library service from any possible criminal activity (Sturges, 2002; Kelehear, 2005). However, references to unacceptable use surpasses elements such as aims and objectives in the AUPs, which occurs in 95 of the AUPs.

Whilst illegal use seemed to be stated in a somewhat standard, if not always descriptive way (often accompanied by a list of legislation), the nature of what counted as unacceptable use varied between AUPs. Causing damages to hardware or software was common, as was users altering computer peripherals or software, or loading their own software. Users disturbing others or upsetting members of staff or other patrons by using foul language was also frequently mentioned. Offensive content and offending others was by far the most mentioned unacceptable usage, and was referenced in 160 AUPs, with 364 references overall. “Obscene” was referenced in 160 sources, “pornography/pornographic” in 25

sources, and “sexual content” in 45 sources. This is in line with findings from the MAIPLE project (Spacey at el., 2014), which found that these breaches of this type were the most commonly occurring in their survey responses. Patrons and usage were sometimes split into legitimate and non-legitimate categories, with the activities of the former having privacy respected during monitoring. This echoes Foucault’s concept of the control being wielded by authorities acting according to a “binary division” (Foucault, 1991: 201). The use of electronic surveillance to decide who is classified as legitimate and who is not also suggests Lyon’s (2003) concept or social sorting; certain users are classified as good and certain users are classified as bad. Obviously the library service must differentiate between what is acceptable and unacceptable use in the public library – not doing so could leave the service liable – however the nature by which this sorting is carried out does suggest binary divisions and electronic categorisation of individuals.

The AUPs started to diverge in areas such as specific Internet usage; some authorities allowed the use of social networks, games, and online transactions, whilst others did not. One AUP did not allow the use of CDs – whether it be games, music, or software. Generally, AUPs allowed but cautioned the use of the Internet for buying goods:

- “Sale and purchase of goods over the Internet is permitted, provided always that: the nature of the goods does not infringe any of the other conditions of use set out here.” (AUP 16)

Some AUPs barred online transactions completely. AUP 139 lists “Online financial transactions” amongst its unacceptable uses and states that:

- "The following actions will not be acceptable and will result in the individual's Internet access being withdrawn and may also result in legal action.” (AUP 139)

Using the Internet to buy goods and services is a common reason for people going online. The library service may seek to prevent users from using the Internet in this way to protect

them from buying goods from a disreputable source, or possibly to prevent criminals conducting business online. Framing it in such a way as to make the decision seem almost arbitrary gives the AUP a heavy-handed and authoritarian tone.

23 sources specifically mention online gambling. Again however, the clarity and detail varies:

- Eight of the sources state online gambling is prohibited due to the library having no license for such activity.
- Five of the sources mention it is prohibited, but do not make any mention of the library service's licensing situation. Of these five, three put it in the same context as illegal activity, pornography, or commercial mailing.
- Six of the sources filter out gambling websites (one AUP filters gambling websites on an "individual basis").
- Two of the sources accept no responsibility if the user participates in such websites.
- One AUP, in which the library service is run by a community trust, prohibits gambling on the basis of the trust's reputation being at risk.
- One AUP mentions the prohibition of underage gambling.

Like financial transactions, online chat is seen as a risky endeavour by some AUPs and users are either urged caution or advised against such activities altogether. Some AUPs distinguish between chat rooms and social networks, allowing the latter but not the former:

- "Certain uses of the computers are prohibited. These are:…
  Access to chat rooms. Access to social networking sites (eg Bebo and Facebook) is allowed." (AUP 109)

Some AUPs prohibited the use of chat room or gaming websites, noting that these are low priority uses of the ICT facilities. 19 AUPs either prohibit chat rooms or heavily restrict them in some way. Five AUPs restrict chat facilities for PCs designated as children only. Four AUPs explicitly state that chat facilities is one of the services the ICT facilities are provided

for. One AUP discusses chat facilities as being an important part of communication and learning:

- “E mail, Chat Lines and Games We do not restrict access to e-mail or chat line facilities, although we cannot guarantee the receipt of e-mail messages. We feel that such restrictions would be detrimental to the idea that learning should be encouraged via different routes. The use of such sites supports the recreational needs of the community and encourages the building of IT skills and confidence.” (AUP 119)

17 AUPs discussed the risks involved with online chat:

- “Avoid:

  Remaining on a site (eg chat room, social media site, blog, instant messaging etc), if someone says or writes something which makes you feel uncomfortable, and report it to staff” (AUP 5)
- “If you feel threatened or offended by discussion in a chat room then you should leave it.” (AUP 57)
- “7) When visiting chat rooms or newsgroups you must not use language that may cause offence, and you must disconnect if such language is used by other chat room participants. Be careful when giving personal contact information in a chat room.” (AUP 99)

AUP 28 listed chat sites along with pornography:

- “Not attempt to access pornography, chat, or other unsuitable sites.” (AUP 28)

Linking a chat room with pornography, deeming it as an “unsuitable site”, and actively encouraging the use of such websites to establish a connection with others are very different ways of framing such facilities. The use of chat room websites was not consistent across the AUPs.

The unacceptable use of facilities was sometimes the very first thing outlined in the AUP. AUP 102 begins with this statement regarding misuse:

- "You must not deliberately search for, or view, pornographic, obscene, violent or racist material or use search terms considered to be obscene, racist, violent or offensive." (AUP 102)

Opening an AUP with such a statement is a rather negative way to begin a document of conditions for the library service. The emphasis on viewing certain types of Internet content could be an important issue for this particular authority; an indication that the IT facilities with this authority have been used for such things in the past and the creators of the AUP hope to curb this with a strong opening statement. Opening an AUP with the words "You must not" does not promote information access, or the library facilities. It is also framed in a way that does not give justification for why this is the case. By stating that viewing violent or racist material in the library could affect other members of the library and staff would perhaps be a more positive approach.

AUPs varied with regards to what was considered appropriate use of the Internet. Chat rooms and streaming television were prohibited by some PLAs and promoted by others. Chat rooms in particular, were framed in very different ways, being encouraged by some institutions as a way to express oneself and connect with others, whilst other AUPs listed chat rooms as a prohibited function in the same vein as accessing websites discussing criminal acts and drug use. The varied stance on chat rooms reflects the uneven nature of the AUPs as a whole, and also highlights the levels of access provided to some patrons that are denied to others. Some AUPs made statements that implicitly link chat rooms with pornographic material and abusive marketing. As Sturges (2002) notes, one of the big draws of the Internet is the connection to other people from around the world. The World Wide Web is a tool for interaction, as well as a resource for information. Chat rooms have received support and derision for their ability to connect people with like minds. The unrestrained, at times anarchic nature of the Internet – the one that allows content creators to upload

whatever they like, and similarly allow others to disparagingly critique said content – is perhaps most exemplified through domains such as message boards, forums, and chat rooms. However, at their fundamental level, these facilities are tools for communication, something that ICT facilities allow that books do not, so it seems strange that a public library should want to deny patrons the use of such facilities. This also highlights the problem of what the Internet should be used for in a public facility. If the scope of access in a public library includes personal and recreational use, it may be seen as arbitrary to deny users access to chat rooms. Chat rooms may be disallowed so that children have better protection against potential contact with strangers, however it effectively denies other users access to possible connections with others over the Internet.

6.2.6 Unacceptable use – protection or care

Some of the references to misuse were explicitly with the aim of protecting or caring for other patrons. Of the 563 references to unacceptable use, 282 references were specifically to protect others. For example:

- “I will respect the privacy and sensibilities of other library users, and I will not cause noise, or display text that may be reasonably viewed as obscene or offensive.” (AUP 3)
- “Users must respect the privacy of others and must not transmit information, photographs or images of another individual without their knowledge and consent through use of mobile phone cameras or otherwise.” (AUP 57)
- “All e-mail must be phrased inoffensively and used for a proper purpose. The following in particular (but not exclusively) are prohibited through e-mail:
  Creating, sending or storing any abusive, offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
  Harassment in any form (including sexual and racial harassment). (AUP 58)

In terms of accessing content in the presence of others, most AUPs stated that users should avoid material that may be offensive, three AUPs also mention embarrassment:

- "Will not use email systems or social networking sites to send inappropriate material or malicious communications to others." (AUP 106)
- "Libraries are used by many different types of customers who engage in many different activities. Please be considerate of other library users." (AUP 145)

These examples protect library users as a whole, but it can also disrupt the individual's freedom of expression. It is not clear what a "proper purpose" is. What is "inoffensive" can also differ and is largely subjective. Again, there is the potential of a chilling effect here, if patrons are unsure what sort of material is acceptable to transmit as part of their ICT access. Freedom of speech is an important part of personal development and citizen participation in a democracy (Fried, 1984; Barendt, 2007), and this is limited for a patron if they are confused by the wording of the AUP. It also means the library service is eschewing individual rights for the overall protection of the community. However, to allow individuals complete freedom of expression, without any restraint, could be potentially harmful to others. The library needs to be socially responsible whilst balancing the rights of the individual, which can become a potential quagmire (McMenemy, 2016). This tension can clearly be seen here, in the often vague wording of the AUPs.

6.2.7 Service commitments

197 of the AUPs outlined what service commitments the library service provides. The use of a disclaimer regarding accuracy of information on the Internet was frequently referenced:

- "The Internet offers unlimited global access to information and [NAME REMOVED] Library & Information Services will not be held responsible for the accuracy, validity, legality or usefulness of information accessed on-line. Nor can it be held accountable for any unacceptable or inappropriate use made by an individual." (AUP 1)

AUP 99 goes a step further:

- "[NAME REMOVED] makes every effort to minimise risks to users of public computers, it is neither responsible nor accountable for much of the material accessible through them. [NAME REMOVED] accepts no responsibility for any financial loss, personal harm, offence or distress caused as a direct or indirect consequence of using its computers." (AUP 99)

By listing financial loss and distress the library service has made sure it is covered if patrons use financial advice from amateur websites or stumble upon information or images that they find shocking. It is important to make sure the patron understands that the information they find on the Internet is not checked for quality or accuracy by the library service however AUP 99 has this statement at the very top of the AUP document. Is this an ideal way of informing patrons about the potentially shocking content they may find on the Internet? Are words like distress perhaps too strong to feature in the opening of a document? This paragraph is at the very start of the AUP – there is no preamble before this disclaimer. Again, with a proper opening statement, outlining the aims and objectives of the library service, the strong wording here could have been tempered.

AUP 187 has a similar disclaimer regarding Internet accuracy and speed, in a positive tone:

- “It should be remembered that the web is a world-wide family of computers and communications links. It is not owned by any one organisation and its speed of operation does vary from day to day.” (AUP 187)

This statement is descriptive, positive (“world-wide family”) and informative to the patron, whilst also being a disclaimer for the library service.

- “All users of the Council’s internet/e-mail facilities implicitly indemnify the Council against any claims, demands, costs, losses or damages that the Council may incur or suffer as a result of any breach of these protocols by users. This means that the Council may seek to recover their costs against a user if those costs are incurred as a result of the actions of a user, which are in breach of this protocol.” (AUP 58)

AUP 58 has taken care to explain the disclaimer further, and what it means for the patron.

Bandwidth restrictions were also cited as a means of allowing for more equal access for all users:

- "[NAME REMOVED] reserves the right to restrict access to sites which are bandwidth-intensive in order to maintain a quality level of service across the network." (AUP 2)

This AUP discusses bandwidth restrictions with a view to providing a better service for all users.

6.2.8 User commitments

A number of the AUPs contrasted the responsibilities of the user with that of the library. AUP 134 separates responsibilities of the user and responsibilities of the library into two different sections, which are clearly headed as such. 20 of the AUPs used a variation of the phrase "As a user, it is your personal responsibility to ensure the accuracy of information you discover" (3 omitted the word "personal")**.** Using "it is your responsibility" rather than the passive voice "users must not" can encourage the user to feel more actively involved in the process. Having a section titled "user responsibilities" rather than simply a list of demands titled "misuse", may sound less authoritarian, and will help the user recognise their responsibilities, thus making the AUP feel more personal. How user commitments were expressed varied between AUPs:

- "Please use our services responsibly and respect the needs of other users." (AUP 153)
- "Whilst using the IT facilities we ask you to act courteously and to respect the needs of other users and staff, in accordance with the Library's Codes of Practice." (AUP 158)
- "Users must not behave in a manner that disrupts other users of library services. In particular:-" (AUP 137)

AUP 137 is phrased in such a way that suggests compliance. AUP 153 and 158 frame it as respecting others or in the interests of the community.

AUP 175 starts off with user commitments – is this too much onus on the user? AUP 175 begins with a disclaimer under the heading “The Internet and Your Responsibility”, whilst this is a good way to encourage users taking responsibility for their Internet usage, perhaps starting an AUP with such a statement puts too much onus on the user, and starts off the AUP in a negative light. AUP 195 only mentions user commitments in terms of disciplinary procedure.

6.3 Filtering

6.3.1 Filtering usage and how filtering is described

Filtering is an important part of managing Internet access in public libraries and any limitations it puts on a user’s information access should be laid out clearly in the AUP. Filtering is a widely used method of managing access, and its use was mentioned in 80% of the AUPs. However, how it was mentioned and how it was deployed varied between the documents.

- 167 AUPs were coded as filtering in use
- 2 AUPs explicitly stated that there is no filtering in use
- 32 sources made no reference to filtering or blocking software
- 4 AUPs were not explicit in their description of blocking websites and as such were coded as unclear

Interestingly, levelled filtering was somewhat clustered geographically – with neighbouring counties tending to share similar approaches. However, they did not necessarily share other features. The two AUPs that explicitly stated filtering not to be in use were not similar in size, nor were they close to one another. Because filtering software blocks access to certain content, it is, by its very nature, prohibitive to access. However, such practices, when used effectively, can also be used to promote information access: patrons may feel safer in the knowledge that their Internet access is passed through a protective barrier, rendering it less

likely that they will stumble upon images or text of a disturbing or pornographic nature. Likewise, guardians may find it easier to let children explore the Internet if they know that their access is filtered. In the 167 AUPs coded as filtering in use, 46 AUPs mention levelled filtering, that is, the amount of content blocked by the software will be dependent on the type of user, for example:

- “The Internet facilities are filtered, with a high level of filtering for children's access and a lower level of filtering for adult users.” (AUP 21)

Five of the sources were coded as having filtering restricted to children only. Some AUPs stated this by noting that filtering is excluded for adults, whilst others stated this by only including filtering in the children’s access section. AUP 60 separated filtering into three separate categories: adult, teenager, and child. Allowing for a more nuanced filtering system helps to ensure older age groups have access that is not blocked unnecessarily by filters, and younger age groups have more of a safety barrier when they are browsing the Internet. Some of the AUPs explicitly stated that the PLA believed library patrons wished for Internet access to be filtered so that extreme online content could be avoided. This is reflective of the MAIPLE project’s findings, which noted that the users interviewed generally supported the use of filtering, especially with regards to children’s access (Spacey et al., 2014). A filtering system that has three levels may allow teenagers to look at websites on topics such as sexual health for example, which may be blocked if they were required to use a computer which had stricter levels of filtering. The levelled approach allows for a more nuanced method of content-blocking. This is not widespread, however, according to the AUP documentation, with only 46 AUPs implementing levelled filtering. It is also, as Skaggs (2003) points out, not a completely effective method of filtering, with filtering limitations such as they are possibly still allowing children access to restricted websites, and the possibility of a child viewing content on a less restricted computer nearby.

The two AUPs that explicitly state that filtering is not in use both allow patrons to have unfettered access, and also protect the library service by explicitly stating that this is the

case. It is however, possible that some users will unwittingly find themselves accessing upsetting websites, and although a statement has been made, patrons may still complain. It is a difficult balance between providing as much access to information as possible, whilst at the same time protecting the service's user-base and satisfying the various stakeholders of the public library. Educating patrons on safe use of the Internet can help to prevent patrons accessing content they may find disturbing, and the steps they can take if they do come across such content. Educating users will help build their confidence when using the ICT facilities, and a strong AUP can help with this (National Research Council, 2002; BECTA, 2009).

Filtering software is characterised as having different uses in the AUPs: it safeguards patrons; it prevents patrons having access to material and prevents material being exposed to patrons; it suppresses materials; it regulates usage; it eliminates material; it blocks websites; and it bars users from accessing certain websites. Four AUPs use the word "suppress" which is interesting considering the negative connotations of the word (such as suppression of information):

- "We cannot guarantee that material capable of causing offence will be suppressed." (AUP 40)

The view that the use of filtering software is a controlling mechanism was echoed in a number of the AUPs that use filtering software:

- "Access is controlled, and content is "filtered" (see below)." (AUP 10)

Some AUPs framed filtering as a response to bad behaviour. After listing actions or behaviour not allowed in the library (for instance exceeding daily allowances of Internet use, or viewing or distributing illegal materials) one source stated that:

- "Failure to comply with the above will result in appropriate action being taken. This may include, covert or overt monitoring, blocking, removal of any potentially offensive

material, injunctive action by the council and reporting the matter to the police." (AUP 113)

Rather than being a preventative measure, filtering has been nestled into a group of actions as a response to bad behaviour, not as a way to protect users.

Filtering is used as a defence mechanism against content that is potentially upsetting for the patron and is used to provide a safe Internet experience, to protect or safeguard patrons particularly where children are concerned:

- "[NAME REMOVED] Council has a filtering policy which helps to provide safe access to the Internet, especially for children and young people." (AUP 23)
- "Children under the age of 12 are encouraged to be library members but are not subject to any charges. Extra filtering is installed on PCs in children's libraries for reasons of Safeguarding." (AUP 29)
- "Users must agree to use computers protected by software that filters content and restrict access to some material and must make no attempt to remove or alter such safeguards." (AUP 104)

Some of the AUPs used the idea of mitigating against a risk or using filtering as a shield to protect users. Other AUPs emphasised the communal nature of the library:

- "We filter sites which are not appropriate in a public library environment." (AUP 48)
- "Our Internet content filter [NAME REMOVED] offer filtered access to the Internet for all users because: We believe the majority of our customers expect us to attempt to ban the most extreme material on the Internet." (AUP 62)

Contrast AUP 62's reasoning (they believe customers expect the library to provide some sort of restriction on extreme material) with AUP 67:

- "Filtering software is in place to prevent access to material on the Internet which [NAME REMOVED] considers inappropriate." (AUP 67)

While AUP 62 puts the library patron as the reasoning behind providing filtering software, AUP 67 states that the decision is down to the authority. There is an interesting contrast here: some of the AUPs state that material considered inappropriate by the council or authority will be blocked, others state it is due to what patrons expect or note that the public library is a space shared by different members of the public, and thus users should expect some sort of limitations on their behaviour.

Filtering may protect the community from criminal activities and inappropriate use of the library facilities, however by doing so, the individual's right to access information free from intrusion into their privacy is lost. Does this mean the library is eschewing individual rights for information seeking and access? Would the overall utility also potentially be raised if access was completely unfettered and filter free? It could be argued that patrons should not have to worry about being confronted by offensive or upsetting imagery when they visit their local library. The public library must provide its service with the visitor in mind and it is perhaps in the public interest that filtering and surveillance are active. Indeed, some of the AUPs explicitly stated this to be the case; that the community would expect access to be monitored in some way. However, this protection from potential distress does provide a form of censorship (McMenemy and Burton, 2005), one that is potentially harmful for access to information. The library has an ethical commitment both to further information seeking and access, and also to the public good. The library also must think of the individual user as well as the community as a whole (Marco, 1993; Trushina, 2004). There is a difficult balance between catering to the public good whilst invading individual privacy by monitoring and filtering. Blocking some information through filtering software will possibly cause a substantial amount of material unable to be accessed.

Other AUPs give no reasoning as to why filtering software is used, or the reasoning is otherwise vague:

- "All Internet access is filtered and monitored. Abuse of the computer facilities may result in the withdrawal of your facilities to use the public computers." (AUP 7)

- "**Security**

  Access to Internet sites is filtered for all users. Access for children and young people under 16 years old is subject to the same restrictions as access in schools, at most times. Library staff cannot be responsible for supervising access by children. Filtering software may also eliminate material that is perfectly acceptable. The library service will consider releasing any such site after careful checking." (AUP 14)

Although information regarding filtering is placed in the "Security" section of AUP 14 and gives some information as to what filtering software does (references to offensive material and releasing websites for example), it seems this sort of information will still come across as rather opaque to someone with limited experience in Internet security measures. It would simply take a quick sentence to describe what filtering software is used for to make the explanation and process transparent. Some of the AUPs provided a detailed list of which websites were considered unacceptable and therefore filtered by the PLA, others contained only references to websites considered "offensive" or "harmful". What could be potentially frustrating for library patrons was the AUPs that gave no reason for filtering at all:

AUP 24 states that:

- "We use software to monitor and filter all use of the internet on public computers. The Wi-Fi service usage is also monitored, including the retention of browsing activity." (AUP 24)

There is no clear explanation as to why the library service filters (or indeed monitors). The AUP follows with a statement reserving the right to sanction users if staff members have a reasonable suspicion of misuse. It is perhaps to be assumed that this is why filtering and monitoring is carried out, but because this is not explicitly stated (a key aspect of the AUP), this cannot be taken for granted. There is no clear reasoning here why this PLA uses filtering software. Stating that the library service filters without clear guidance on why it does so, what filtering software actually does, and what criteria it works under may serve to

discourage users from accessing information. The way filtering has been described here does not even suggest its usage as a means of protecting the library's user base. Instead it is linked with surveillance and retention of browsing activity which points more to crime detection. Overall, this may serve to protect the library's patrons from those users who are accessing or distributing illegal content or using the library ICT facilities for criminal activities, however the phrasing of this statement does nothing to suggest that, and thus does not promote information access.

In a public institution, one that houses adults and children alike, it might be implied that completely unfettered access to the Internet is not an option. However, any restrictions that the public library puts in place should be reasonable and communicated clearly to the patron, with guidance to further information points if necessary. AUP 118 has given a clear description of what filtering is, why it is there, and what it does:

- "Filtering is the term used to describe the use of software which restricts access to certain types of material on the Internet. Such software is used to restrict access to sites that for example contain pornography and other potentially offensive content." (AUP 118)

Filtering was described with varying levels of detail, with some AUPs going into depth about the software, including listing which types of websites will be filtered. Whilst some AUPs give scant description or explanation of what filtering software does or which material it blocks, others went into more detail:

- "It is the policy of [NAME REMOVED] Council to use content filtering routines to block access to websites on the internet which the council judges to be inappropriate…

  Some file types are blocked in order to minimise the spread of viruses onto our system. These include some executable, compressed, JavaScript, VBScript, audio and video file types.

A full list of blocked file types is available on request.” (AUP 9)

Other AUPs included an appendix that listed the types of website or content that would be blocked or not blocked by the filtering software. Whilst a comprehensive list might be too time-consuming for the patron to read in the main body of the AUP, providing an appendix or a list on request allows for the patron to have more information if they desire and it allows for the filtering process to be more transparent.

Filtering was also referred to as “specialist software”:

- “Accessing sites deemed inappropriate, offensive or illegal will not be permitted. Specialist software is in place to record access to, and bar viewing of, such sites.” (AUP 133)
- “Access to sites deemed to be inappropriate, offensive or illegal will not be permitted under any circumstances. Specialist software - continually reviewed and updated - is in place to record attempted access to, and to bar viewing of, such sites.” (AUP 28)
- "The libraries use proprietary filtering software to reduce the risk of access to inappropriate internet sites and content." (AUP 201)

The explicit reference to the recording of such websites, and also the reference made to the fact that the filtering reference list is continually updated could serve as an added deterrent. It could also be used to reassure parents or guardians that the software the library uses is proficient.

Some AUPs mentioned filtering was in use at the very beginning of the AUP:

- “Our aim is to make available to our users as wide a range of information as possible, including free, filtered Internet access.” (AUP 116)

Of the two AUPs that explicitly stated filtering was not used, AUP 50 states:

- “You should also be aware that blocking and/or filtering systems are not used to control Internet access” (AUP 50)

AUP 61 explicitly states that filtering is not used on either adult or child PCs:

- “Filtering and monitoring policy

  11. Access to the Internet in all areas of the library designated for adult and children’s use is unfiltered.

  12. Staff may monitor your use of the Internet at any time.” (AUP 61)

Although the Internet is not being filtered, the library service still uses monitoring to manage access. It is not clear why this monitoring is taking place, however.

6.3.2 Filtering use is unclear or not mentioned

Filtering was mentioned to be in use in 80% of the documents. Whilst this number is high, the two PLAs that did not use filtering explicitly stated this to be the case in the AUP, and of the 37 remaining AUPs, 31 made no reference to filtering at all, and six were coded as unclear. Studies by the MAIPLE project (Spacey et al., 2014; Spacey et al., 2015) and Brown and McMenemy (2013) have found filtering to be a widely spread practice, which raises the question if the PLAs represented by the AUPs truly do not use filtering or have simply failed to mention it. It is important that practices such as filtering be made explicit in policy documentation (Sturges, 2002), so this is perhaps a worrying find. This lack of clarity is reflective of the MAIPLE project which found that half of user interviewees in their public library case studies were unaware that the library used filtering software (Spacey et al., 2014: iv).

It is interesting that several AUPs make no reference to filtering software, when it has been indicated by other studies that filtering websites is a widespread practice in UK public libraries. Declining to mention that some content will be blocked, or that measures are in place to prevent users from accessing potentially offensive content seems an oversight. Sturges (2002) notes that any restrictions to accessing information such as the use of filtering software should be made clear to the patron. Some of the AUPs discourage access to information due to their vague statements on filtering practices, such as the efficacy of filtering, and what patrons should do when they come across a blocked website that they

think should be accessible. For filtering to have a positive effect, it must be deployed effectively, in such a way that encourages access, and its usage is explained in a clear manner. Some AUPs simply did not make any mention of filtering software, whilst others made references to websites being unavailable.

- "[NAME REMOVED] Libraries and Information Service is able to control and monitor user website access in line with our security requirements however you are responsible for the sites you chose to visit." (AUP 126)

This statement is very vague. The mention of the library service being able to "control and monitor user website access" does suggest some form of filtering is in place, however it is not wholly clear for the user.

- "[NAME REMOVED] Libraries' decision as to which websites fall into these categories is final. Users should be aware that [NAME REMOVED] monitors Internet use and some sites will be blocked." (AUP 177)

This last example is also quite vague; it is clear that the library is using filtering software to monitor and block websites, however to those not proficient in Internet use, this is not very well explained. Whilst there may be limited space in the AUP to try and encourage users to read the document, readers must still be supplied with sufficient information for them to understand what sort of service their library is providing them with.

One AUP does mention the use of monitoring patrons:

- "The library will monitor Internet and e-mail use to ensure the use of the facilities is made in accordance with the conditions of use set out above – and for this purpose only." (AUP 169)

Further down the page, the AUP states that:

- "If you alight on a site which you consider may be offensive to other users or receive e-mail which may be considered offensive if viewed by other users please alert a

member of staff who will take the appropriate action to prevent further access." (AUP 169)

Prior to this, the only reference to any possible filtering was the initial statement regarding monitoring patrons. It is not clear however, that this monitoring will include filtering. It is recommended that if filtering is being used in the library, then it should be explicitly stated that this is the case.

6.3.3 The efficacy of filtering software

Filtering, as it has been discussed, is not always a fool proof method of blocking potentially harmful content. 118 of the AUPs note that filtering is not guaranteed to be 100% effective. Some AUPs hinted at this idea, but did not explicitly state it outright, and thus were not coded as having informed patrons of such. For example:

- "Although the Council filters inappropriate material, these services cannot be held responsible for the content, accuracy or quality of the information retrieved. If you choose to use the internet, you should not access, create or transmit anything that is designed to, or likely to, cause offence or needless anxiety to anyone. Transmission of any material in violation of any laws is prohibited. This includes, but is not limited to, copyright material, threatening or obscene material, pornographic material or material protected by trade secret.

  Please note that any continued attempt to access a site displayed as inaccessible will result in the system shutting down the computer and alerting library staff. If you require access to a barred site, please contact a member of staff." (AUP 5)

This source is too vague as to why someone would need to request access to a barred site. It is not completely clear that websites made inaccessible by the filtering software may have been made in error. Compared with these extracts:

- “Some legitimate sites may be blocked as a result of the filtering activity and other inappropriate sites may inadvertently be made available prior to their being blocked.” (AUP 8)
- “The filtering in use can sometimes inadvertently block sites which are not inappropriate and can also sometimes allow access to sites containing material that would be deemed to be inappropriate.” (AUP 9)

AUP 8 and 9 give a concise account of how filtering software may approve websites that should be blocked and erroneously block “safe” websites.

Some AUPs use filtering in conjunction with physical monitoring by staff to ensure a more comprehensive level of protection:

- “Filtering can never be 100% foolproof so library and record office staff are also watchful and will remind people who look at offensive content that this is not appropriate and that, if they do not stop, they may have their sessions closed down, and in some cases have their internet access taken away for a time.” (AUP 171)

This AUP discusses the efficacy of filtering software and outlines the library service’s use of monitoring to support this method of access management. By using filtering in conjunction with monitoring managing access to the Internet is strengthened. However, the AUP does not give any further information on what to do if a patron accesses a website that the filtering software has categorised incorrectly.

6.3.4 Unblocking

Of the 166 AUPs that state filtering is in use, 66 have information regarding how to unblock websites. The process of unblocking websites usually required the patron contacting a member of staff:

- “If you find a site that is blocked and you think it should not be blocked, please fill in the online form or write down the web address (URL) and any error messages that

appear. Give these to library staff so that we can investigate. Please note that it may not be possible to enable access." (AUP 12)

- "Filtering software may also eliminate material that is perfectly acceptable. The library service will consider releasing any such site after careful checking." (AUP 14)

For some of the AUPs, perhaps there an assumption has been made that if an Internet user comes across a website that they cannot access, despite being on a subject that they would deem inoffensive, the user will simply make an enquiry with an available member of staff. However, if the information regarding unblocking content is not there, then it should not be assumed that the library patron will know what to do. This reflects the findings of the MAIPLE project, where unblocking procedures were noted as being inconsistent (Spacey et al., 2014). Whilst filtering may be an important part of managing access in public libraries, especially when it comes to protecting more vulnerable users such as children, appropriate information should be provided in the case of webpages that are blocked to the patron which do not fall under the filtering settings, or if a patron is confronted with a webpage that should have been blocked by the filtering software. Not informing the patron of unblocking procedures risks the patron not being able to access information that may be perfectly legitimate, and thus does not promote access to information.

The idea of checks was reflected in several of the AUPs:

- "If you cannot access a website as it is blocked, please speak to a member of staff to request it be released for access (subject to checks)." (AUPs 16)

The use of words such as "investigation", "careful consideration", and "checking", evokes subtle gatekeeping and power by the library service.

AUP 190 states that:

- "Filtering software is used to restrict access to sites that [NAME REMOVED] Council deems inappropriate and/or offensive. The effectiveness of any filtering software

cannot be guaranteed and any user can recommend that access to a particular site can be permitted or denied." (AUP 190)

The use of the word "recommend" suggests a communal, shared library service**.**

- "Filtering All access to the Internet in libraries is filtered but we cannot guarantee that all offensive sites will be blocked. Equally, some acceptable sites may be incorrectly blocked. What may be acceptable or unacceptable to one person may not be to another, but if you find a site which you think should be blocked or unblocked, please inform a member of library staff. [NAME REMOVED] Council will decide on what action to take." (AUP 46)
- "Filtering All access to the internet in libraries is filtered but we cannot guarantee that all offensive sites will be blocked. Equally, some acceptable sites may be incorrectly blocked. What may be acceptable is a personal view but if you find a site which you think should be blocked or unblocked, please inform a member of staff. [NAME REMOVED] IT Services will decide on what action to take." (AUP 31)

The AUPs both note that personal tastes vary but encourage users to inform staff if they feel a website has been wrongly categorised.

- "A filter system is used on the library computers which restricts access to websites that are inappropriate and/or offensive. If you feel that the website you wish to access should not be restricted, please inform one of the staff. If necessary your concerns may be discussed away from the public area." (AUP 154)

This AUP has taken the approach of allowing the user to talk to a member of staff with some privacy. This could work well for patrons who may be looking for information on sensitive subjects such as matters relating to health or sexuality. CILIP's eighth ethical principle is "Respect for confidentiality and privacy in dealing with information users." The library authority has clearly taken that into consideration when creating the AUP: patrons are able to feel confident that their concerns may be expressed in privacy. Whilst a patron in any

library authority can ask the library staff to discuss matters in a space away from the main library area, not every patron will feel confident enough to ask this, and AUP 154 gives reassurance to patrons who may not have had the confidence otherwise.

Similar to studies by Willson and Oulton (2000), Brown and McMenemy (2013), and the findings of the MAIPLE project (Spacey et al., 2014; Spacey at al., 2015) a number of the AUPs stated that filtering decisions were not in the hands of the library staff members, instead the decision is decided at the local authority level:

- "The Council – not library staff – decides what content the public can and can't see and what should be filtered… If you think that a blocked website should be accessible or that a website should be blocked, please put your request to a member of staff. The Council will then review this. FTP sites are generally restricted by our firewall and libraries have no control over this. However some FTP sites may be available." (AUP 89)

Again, it is the Council or IT staff who will decide on what action to take, not specifically the library staff. It is of concern that several of the AUPs state that it is the local authority, and not the library's decision regarding the use of filtering. The local authority also has the means to block or unblock specific websites. This may be a logistical issue – the IT team may be housed in a separate location from the library – however, as with the selection process for the library's reading materials, what is to be viewed or hidden by the library's filtering system, should come down to the library itself, and not from an outside group. The role of the librarian is to disseminate information, select which books are to be housed in the building, to catalogue them appropriately, and to help the reader locate the information that they seek. The librarian cannot carry out their duty effectively if they are prevented from making the decisions themselves. Not providing an easy way of passing filtering software if it is in error can lead to the software becoming a passive "instrument of censorship" (Brown and McMenemy, 2013: 198).

Proving that a website is of academic use to a librarian exhibits a display of power and was also a subtle display of gatekeeping that was a feature of some AUPs:

- "Users who have a legitimate need to visit normally prohibited sites may be able to do so if they can prove to the Principal Librarian or designated staff that it is for professional or study purposes." (AUP 104)

Statements such as this gives the library an image of gatekeeping. Whilst showing the staff members that the website they wish to use is not harmful or goes against the filtering parameters seems straightforward enough, the language used here is authoritarian and controlling. Having to prove to staff that the website they are using – what sort of proof do they require? – is not wholly clear. The statement also makes a pointed differentiation between legitimate use and other use, which promotes the library as a place to study, rather than as a place to recreate. This is perhaps the conditions under which the use of this particular PLA falls under, but does that not perhaps make it unfair that some PLAs allow their library for recreational use, whilst others only allow their library service for study purposes only?

AUP 182 gives a simple but thorough explanation of unblocking:

- "Web filtering is not an exact science and you may come across a website that you believe to be incorrectly blocked. The [NAME REMOVED] team realise that it is inconvenient and frustrating when a website is blocked for no apparent reason. A process has been set up to allow sites to be vetted and potentially added to a safe list.

  If you want to access a web site that you believe to be acceptable but the site is blocked through web filtering, then please complete the IT Contact Form and your request will be investigated and you will be notified of the outcome." (AUP 182)

As well as unblocking websites, AUPs also gave information on websites that erroneously pass the filtering software:

- “Internet access is filtered and monitored to block inappropriate and illegal web sites or pages. Children and teenagers have different and stricter levels of filtering to adults. We expect parents to take responsibility for their children’s internet browsing in the library, and can block this at a parent’s request.” (AUP 171)

AUP 202 notes that filtering may not be 100% effective, but focusses on blocking more sites rather than unblocking sites:

- “Computers in our libraries use filtering software to help prevent access to the majority of undesirable or objectionable sites. The software is updated regularly to include new sites, but like other products, cannot provide 100% control or guarantee to block all sites due to their constantly changing nature and locations.
  Should you accidentally encounter a site you think should be blocked, please inform library staff of its location address and the reason you think it should be blocked. Staff will then arrange to review the site.” (AUP 202)

This provides a clear explanation of potential problems with filtering software, and how to rectify them. The AUP should however explain this works for unblocking websites as well as blocking them.

A public institution such as the library has to take all of its users into account and must be sensitive to the needs of younger and more vulnerable users (Young, 1997). Filtering has been regarded as a simple and effective solution to protect users from accessing extreme and disturbing content and can help to reassure those patrons who may be worried about inadvertently accessing such content (Willson and Oulton, 2000; Auld and Kranich, 2005). Indeed, this was communicated by some AUPs, stating that they believed patrons want an environment where Internet access is filtered. However, in order to protect the interests of its overall user base, inevitably individual users wishing to access certain materials will lose out.

This is further exacerbated by the lack of control some of the libraries have over the use of filtering software, both on an individual basis, and more generally. Some AUPs note that

there is a lack of control due to the software being implemented via the local authority, rather than the individual library service. There is also the wider issue of the fact that filtering has already selected material, rather than library staff. Filtering is a type of selection process, and it may be likened to the way in which library staff members select which books the library carries. However, where a librarian may have limited space, and needs must make some sort of selection process to ensure a wide variety of reading materials are available for patrons, there is no such limitation on the World Wide Web. There is a question therefore, whether the library should be employing filtering software at all, when it is an institution devoted to information access and dissemination. Filtering is indeed a selection process, but it is also one that may be out of the librarian's hands. A librarian can walk through the stacks and observe patrons at their desks in a similar way that they watch a user's computer screen. The ethical quagmire is the same, but the technology does compound the issue.

Filtering can be both promotional and prohibitive to information access. The AUPs analysed did not tend to give enough information about filtering software or what it does, and what to do if it does not work correctly. Likewise, filtering can be both caring and controlling depending how it is framed in the AUP documents. Filtering was used as both a preventative and responsive measure; as a block to possible disturbing content, or as a response to misuse. Statements were framed in both caring and controlling ways. Some AUPs framed filtering as a defensive mechanism against unwanted, potentially offensive content, which is a caring way of explaining how the software is used. Others however used filtering as a way of controlling users, with some specifically describing content as being controlled, or as a punitive measure for those users not complying with the terms of the AUP. Framing filtering as a method of safeguarding users or helping to protect the community from accessing disturbing material or bandwidth-restricting websites that would mean a poorer service overall is a caring way of describing filtering as a punishment, rather than being regulatory and on the controlling side. This use of filtering can also help to reassure patrons wary of accessing illegal content (Willson and Oulton, 2000).

6.4 CILIP's ethical principles

Access to information is promoted in the AUPs through references to CILIP's ethical principles. In particular, Principle 1 ("Concern for the public good in all professional matters, including respect for diversity within society, and the promoting of equal opportunities and human rights") and Principle 3 ("Commitment to the defence, and the advancement, of access to information, ideas and works of the imagination") are both well represented in the AUPs. CILIP's ethical principles encompass a variety of topics, some of which are staff-specific and so were not expected to be well represented in the AUPs. Principle 11 for example – "Commitment to maintaining and improving personal professional knowledge, skills and competences" – will be of more relevance to library staff than it is to library patrons. AUPs that featured one CILIP principle tended to feature others, and there was a significant overlap with Sturges' essential features.

6.4.1 Principle 1: Concern for the public good in all professional matters, including respect for diversity within society, and the promoting of equal opportunities and human rights

The most represented of CILIP's ethical principles is the first, which states: "Concern for the public good in all professional matters, including respect for diversity within society, and the promoting of equal opportunities and human rights". Principle 1 appeared in 202 of the sources. It had both the largest number of references and also appeared in the largest number of sources overall. The only AUPs that did not feature this node were those that listed the available services, and did not speak to the patrons' use of such. Principle 1 manifested most often in AUP statements regarding supporting the needs of the community:

- "If you are not familiar with the internet, library staff will help you get started and will help you search for information." (AUP 173)
- "The following policy has been developed in order to safeguard both users and their interests." (AUP 1)

- “If you have special needs for accessing the computers, please let us know and we will do our best to help you.” (AUP 25)

It is positive that so many AUPs feature this ethical principle, however, it also highlights the tension in the AUPs between caring and controlling access management. For example, the right of privacy, which is an important part of access to information and freedom of expression: without privacy, the user will not have the full ability to be able to explore information freely. It is a cornerstone of the information profession (Sturges et al., 2001; Woodward, 2007; Gorman, 2015), with privacy being an important ethical concern within library associations internationally (McMenemy et al., 2014). Privacy is a human right, and as such should be respected the library service. It is clear that patron privacy is being invaded in the public library, as surveillance is heavily referenced in the AUPs. Some of the AUPs tried to remain transparent and open with the patron – acknowledging the use of technology that cannot guarantee their privacy. The user is fully informed of a loss of privacy, however statements such as those above, and those regarding privacy and monitoring highlight a clear tension in the library service between trying to fulfil the ethical principles as stated by CILIP, alongside various uses of monitoring technology.

6.4.2 Principle 2: Concern for the good reputation of the information profession

Principle 2 is: “Concern for the good reputation of the information profession”. It was not expected that this would be widely represented as it pertains to how the information profession treats itself rather than its patrons. Nevertheless, Principle 2 was highlighted in some AUPs:

- “The Libraries and Arts Service recognises that it is only through continued public confidence in the upholding of data protection principles that confidence in the library itself can be maintained, which is vital to the library’s role in the community and the community’s right to know.” (AUP 87)

This exact statement was echoed in one other AUP. Although the Data Protection Act was referenced by a number of AUPs, only two AUPs made a point of stating their commitment in this way.

Interestingly, another reference was made to the reputation of the Trust responsible for the public library, but referenced the patrons rather than the information professionals:

- "The following are not permitted:… Using the [NAME REMOVED] Internet facility for the purposes of gambling where the reputation of the Trust may be at risk." (AUP 63)

6.4.3 Principle 3: Commitment to the defence, and the advancement, of access to information, ideas and works of the imagination

Principle 3 covers "Commitment to the defence, and the advancement, of access to information, ideas and works of the imagination." This ethical principle appeared 345 times in 165 of the AUPs. Principle 3 has some overlap with Principle 1 in the AUPs, as commitment to access to information and promoting equal opportunities are both present in AUP statements about provision of learning and information resources:

- "The use of computers is an integral part of the services provided by [NAME REMOVED] Libraries and they can be used to access information, reader development, citizenship, cultural, entertainment and learning resources… The provision of information is one of [NAME REMOVED] Libraries' core services and the access to information using electronic means is part of the library's core service." (AUP 10)
- "[NAME REMOVED] Council provides public access to Internet services for its citizens and customers as part of its objective to ensure the maximum amount of access to knowledge, information and collaboration by its citizens and customers." (AUP 12)

- "[NAME REMOVED] provides public access to the Internet in keeping with its role as a source of information, intellectual development and to help meet the digital inclusion agenda." (AUP 200)

Children's access was generally encouraged, although the parameters for doing so varied between the AUPs in terms of age of access and how much guardian supervision is required.:

- "Children are actively encourage to use the internet. As is the case with all library materials, any restriction of a child's access to the internet is the responsibility of parents or legal guardians. Filtered access is provided on all PCs in the children's libraries and we recommend only high quality websites." (AUP 174)

80% of the AUPs demonstrating a commitment to Principle 3 is encouraging in terms of user access to information and freedom of expression. It should be a priority of all PLAs however, to make sure statements promoting access to information are included in their AUP documents. Some of the documents essentially read as a list of what the library service offers the patron in terms of facilities – whilst this is helpful, there should be encouragement in the AUP to make effective and rewarding use of the facilities. It should not be taken for granted that the patron knows all the facilities that the library's ICT service provides, and statements encouraging access and use of such services can help users make the best use out of the library service (McMenemy, 2014) and could make for a more readable AUP. 40 of the AUPs made no reference to Principle 3 – primarily because they did not establish accessing information as a core part of the service. Rather, the AUP listed what the user could and could not do or took a minimal approach to describing the service.

Like CILIP's first ethical principle, the positive references to access to information also come into conflict with the uses of monitoring technology such as filtering, which ultimately may have a deterring effect on a user's browsing habits.

Access was mostly free across AUPs, with many AUPs explicitly stating this fact. 20 AUPs stated that fees applied to access. Of these:

- Five AUPs stated that charges applied to both library members and non-library members alike (either by a single payment or an annual subscription fee).
- Eight AUPs stated that access is free for library members, but that charges applied for non-members and visitors.
- Two AUPs stated access is free for the first initial time slot, however patrons wishing to use facilities for longer than the initial slot would have to pay a fee.
- Two AUPs stated fees would apply for users wishing to book a specific time slot.
- One AUP stated if library members forgot their library card they would need to pay for access.
- One AUP stated charges applied to group use of ICT facilities.

Although only a small number of PLAs mention charging for facilities, this varied nature of access goes against the library service encouraging equal access to information, and echoes McMenemy's description of a "postcode lottery" (McMenemy, 2014: 11) in terms of service provision. It seems unfair that patrons have to pay for access just because of where they live. Considering the public library's role in the digital divide access should be encouraged for all library patrons, and by creating a pay barrier, some library users will inevitably lose out.

6.4.4 Principle 4: Provision of the best possible service within available resources

Principle 4 is "Provision of the best possible service within available resources." This was mostly referenced in statements of commitment to access provision and ensuring resources were spread amongst users to allow for fullest possible access. 126 of the AUPs referenced Principle 4.

- "Please ensure that you have completed your session within your allotted time in order that all users can enjoy this facility to the full." (AUP 41)

- “The [NAME REMOVED] Council Library and Information Service is committed to the provision of access to information and resources for the wider community in whatever format is most appropriate.” (AUP 58)

AUP 41 frames the use of time limits in a way that highlights how important it is to give other users access.

6.4.5 Principle 5: Concern for balancing the needs of actual and potential users and the reasonable demands of employers

Principle 5 is “Concern for balancing the needs of actual and potential users and the reasonable demands of employers.” The AUP document would not necessarily be expected to cover what an employer demands from the library staff, however it was still represented in a few of the AUPs:

- “When making decisions on blocking access to websites, [NAME REMOVED] Libraries recognises the need to reconcile the conflicting values of maintaining and defending freedom of access to information, protecting others from harm, and obtaining best value from the Council’s investment.” (AUP 84)

6.4.6 Principle 6: Equitable treatment of all information users

Principle 6 is “Equitable treatment of all information users.” This ethical principle was featured in 108 of the AUPs. This principle has overlaps with Principles 1 and 3; promoting equal opportunities, commitment to access, and equitable treatment all share qualities in statements directed at information provision and access for individuals, communities, and visitors.

- “All members of the public are entitled to use the computer facilities provided by [NAME REMOVED] Council at the designated sites. The Council believes that the public are entitled to access the Internet for their informational, educational and leisure needs on payment of the appropriate fee (where applicable).” (AUP 7)
- “Access to the Internet is open to members of the public and is free.” (AUP 100)

Whilst this principle is widely featured in the AUPs, it again highlights the tension between striving to offer access and to treat everyone equally, whilst also using language that divides users into those that are legitimate, and those that are not. Also, as mentioned previously, by charging members for use of the ICT facilities, some members will end up losing out.

6.4.7 Principle 7: Impartiality, and avoidance of inappropriate bias, in acquiring and evaluating information and in mediating it to other information users

Principle 7 is "Impartiality, and avoidance of inappropriate bias, in acquiring and evaluating information and in mediating it to other information users." Principle 7 is another principle that is more witnessed in staff's actions, rather than in the AUP itself and was coded in one of the AUPs:

- "[NAME REMOVED] provides public access to Internet services for its citizens and customers as part of its objective to ensure the maximum amount of access to knowledge, information and collaboration by its citizens and customers." (AUP 12)

6.4.8 Principle 8: Respect for confidentiality and privacy in dealing with information users

Principle 8 is: "Respect for confidentiality and privacy in dealing with information users." This node was referenced in 44 of the AUPs. Again, Principle 8 may be another ethical principle more likely to be observed in the library staff's actions rather than the AUP, however 44 is still quite a low number considering how important privacy is for library users. A number of the AUPs that contained references to privacy mentioned the Data Protection Act and how it affects user data and how the library uses and stores this data. Whilst this is encouraging, it is interesting that this was only referenced in some of the AUPs (21%). The Data Protection Act is an important piece of legislation that is relevant to the information profession and affects the public library and its users. If it is important enough to be referenced in some AUPs, should it not be referenced in all the AUPs? Even a passing reference could be supplemented with information in an accompanying appendix. This is similar to findings by

Sturges et al. (2003) who noted in a survey of libraries in higher and further education, that privacy concerns were not a high priority amongst staff, nor in terms of policy.

Sometimes Principle 8 was referenced as part of the library's monitoring policy, for example:

- "We may monitor your use of the computer, including websites visited, in order to plan better services and to ensure you keep to this policy. We will not use personal information for any other purpose, or divulge it to other people or organisations, in accordance with the Data Protection Act 1998." (AUP 4)

The latter half of this paragraph assures the user that their data will be handled in a safe way, however it is only referenced as part of the overall monitoring policy. A number of the AUPs only mentioned the handling of user information in reference to the library service's monitoring of patrons:

- "[NAME REMOVED] respects users privacy whilst using the Internet, but users should be aware that Internet access is monitored and that random checks will be made on the sites visited. The Library keeps a record of every Web page accessed." (AUP 22)

The issue of trying to balance the privacy needs of individual users against safety concerns for users in general, as well as the library service's IT system, was apparent in a number of the AUPs that discussed user privacy. AUP 73 makes a point of reassuring users that privacy is important, and that privacy invasions will only occur when necessary to protect users:

- "The County Council respects the right of individuals to privacy of communications. At the same time it has a duty to protect the interests of itself and others against unlawful use of its computer facilities. To balance these needs, interception of personal and private communications will not normally take place unless grounds exist to show evidence of some crime or other unlawful or unauthorised use." (AUP 73)

AUP 73 mentions privacy in reference to monitoring, but makes sure to justify any invasions of privacy, which helps to underscore that the service takes user privacy seriously and will only use a patron's information when absolutely necessary for the safety of others. Again, there is a tension here, with trying to protect user privacy, whilst also using technology that invades privacy.

AUP 101 explicitly references the library service and its relationship with users in regards to privacy:

- "[NAME REMOVED] recognizes the position of special trust that libraries have with members of the public. This statement clarifies policy and practice with regard to confidential information about users (and their use of library resources) that comes into [NAME REMOVED]s' possession." (AUP 101)

By acknowledging the storage and use of private information about patrons that libraries have, and speaking on this subject, AUP 101 helps to give assurance to patrons who may be concerned how their data (especially their digital data) is stored and used. AUP 101 then goes into further detail:

- "Therefore, [NAME REMOVED] have adopted the following practice concerning the disclosure of information about library customers. None of the following shall be given, made available or disclosed to any other proper authority without valid legal request in writing:
    - personal details given on joining or when making an enquiry;
    - information about material borrowed;
    - correspondence or information about enquiries made;
    - the frequency and content of Internet use;
    - the frequency or nature of a customer's lawful visits to the library or
    - any other information supplied to the library (or gathered by it)." (AUP 101)

By giving further details about how patron information is used, the library service is being clear and transparent about how it uses patron data, and shows that it takes the privacy of its users seriously.

Privacy was also framed as something that users should be aware of, rather than the staff themselves:

- “Users should abide by copyright laws and licensing agreements and respect the privacy of other users.” (AUP 42)

6.4.9 Principle 9: Concern for the conservation and preservation of our information heritage in all formats

Principles 9-12 pertain more to the librarians themselves, rather than users, and thus were not expected to feature heavily in the AUPs. There were some references to them however. Principle 9 is: “Concern for the conservation and preservation of our information heritage in all formats.” Principle 9 was usually referenced in regards to maintaining the functioning of computers:

- “3. Users may use only software provided for the purpose by [NAME REMOVED] Libraries and must not alter, amend or delete any of the programmes or settings already resident on the computer's internal fixed disk or in its memory.” (AUP 15)

6.4.10 Principle 10: Respect for, and understanding of, the integrity of information items and for the intellectual effort of those who created them

Principle 10 is “Respect for, and understanding of, the integrity of information items and for the intellectual effort of those who created them.” Principle 10 mostly pertains to the responsibility of the library staff to information items. However, it was referenced in regards to copyright. 82 of the AUPs were coded with Principle 10:

- “Copyright

> The scanning of copyright material is only legal for the purpose of private study and/ or research and for other non-commercial purposes. In all other cases prior permission from the copyright owners must be obtained by the user. Wherever possible the source of the material should be acknowledged." (AUP 12)

By making sure the patron is aware of their responsibility towards copyright, the library service ensures they are committed to respecting the intellectual effort of content creators. Some AUPs only mention the actual legislation, without further explanation. It is questionable if the user will truly understand the regulations covering the use of copyrighted materials when it is framed in this way.

6.4.11 Principle 11: Commitment to maintaining and improving personal professional knowledge, skills and competences

Principle 11 is "Commitment to maintaining and improving personal professional knowledge, skills and competences." Principle 11 is another of the ethical principles that would not be expected to be present as much in the AUPs, since it pertains to staff more so than patrons. It was however, represented in one of the AUPs:

- "Our aim is to widen participation, support lifelong learning, provide information in a wide range of formats and give equal access to all users. We are also committed to an ongoing staff training programme which will respond to the needs of internet users." (AUP 117)

This is a reassuring message from the library service – reinforcing the idea that the library service wishes to widen access to the Internet, and having an ongoing training programme for staff makes a commitment to providing such access.

6.4.12 Principle 12: Respect for the skills and competences of all others, whether information professionals or information users, employers or colleagues

Principle 12 is “Respect for the skills and competences of all others, whether information professionals or information users, employers or colleagues.” Principle 12 pertains more to staff than to patrons, and as such was not found in any of the AUPs.

6.5 Conclusion

The panoptic principle was seen to be exhibited in the public library AUPs. Access to information was encouraged through expressions of CILIP’s ethical principles but discouraged through authoritarian language regarding compliance and misuse, the use of possibly intrusive surveillance techniques such as real-time monitoring with pop-ups on user screens, and the inconsistent application of filtering and lack of explanation regarding its use, efficacy, and what to do if the software is in error. The high difficulty regarding the documents’ readability also discourages use of the facilities and was a cause of concern regarding the AUP as a contractual document. This reflects other studies that have similarly found complex and authoritarian language in AUPs. The study both reflected other research that found similar results regarding the application of filtering, and also highlighted the lack of information, considering how many public libraries use the software, and its lack of presence in some of the AUPs. Balancing public access to the Internet whilst also trying to ensure patrons have a safe and pleasant experience using the World Wide Web is difficult, and this was expressed through the varied ways the AUPs discussed and tackled issues of misuse, scope, and monitoring.

This chapter discussed the qualitative findings of the study, as well as place it in the research context found in the literature review. The next chapter will present the model AUP, as developed through the findings of this study.

7 Model policy

7.1 Introduction

The researcher has synthesised all the information gathered in this study to create a model AUP. There is no real reason the UK should not have a single AUP. Access should be equal, and a single, robust AUP would reflect this. This study has found public library AUPs to be very varied and inconsistent, which reflects other studies such as the MAIPLE project, which noted the "lack of standardisation or harmonisation across services with regard to Internet provision" (Spacey et al., 2014: 89). An important part of combatting this could be a single AUP, fit for all public library access. This research has found that some authorities do clearly share AUP formats – in neighbouring PLAs there was sometimes clearly a shared template. In this same way a national AUP, or at least a national model for an AUP, could allow for best practice and allows for a more sustainable service overall. As part of their recommendations, the MAIPLE project states that there is "a need for a more unified and consistent approach to managing Internet access based on nationally agreed guidelines" (Spacey et al., 2014: v). A model AUP could allow for a more standardised service across the country. As well as a sustained effort in constructing such a document, there is also the equality that patrons should expect. Having a single, strong document supports both the information professional, and the service itself: "By a collective pooling of effort and an agreement on service standards we could create a document that is widely understood and could act as an advocacy tool for the services we provide" (McMenemy, 2014: 11).

This policy is largely based on Sturges' essential elements of an AUP, along with other guidance from *Public Internet Access in Libraries and Information Services*. Although Sturges' elements are from 2002, they remain effective core principles because they are based on the fundamental principles upon which ICT access should rest upon. Sturges created these principles through an examination of best practice in the literature. Alongside this, there is a general lack of material regarding the formation of AUPs (McMenemy, 2014).

As noted before, Sturges states that an AUP should have seven key elements: aims and objectives; eligibility; scope; illegal use; unacceptable use; service commitments and user commitments. Along with this, the AUP should have clarity and be direct in its approach, which will instil confidence in patrons and staff alike, and should avoid vague and unnecessarily complicated wording, which will inhibit understanding and consequently make the document weaker. Alongside this, research from the AUP section in the Literature Review chapter was also consulted, along with the discoveries made by analysing the AUPs gathered for the study.

7.2 The title

Sturges has noted that the term “acceptable use policy” is somewhat loaded: what is acceptable to one person may not be acceptable to another, and which entity defines what is acceptable and why should they be the arbiters of this? Sturges has instead suggested “Internet use policy” as a more neutral alternative (Sturges, 2002). Leading with ‘acceptable use policy’ does put the emphasis on a dichotomy between what is acceptable and what is unacceptable, immediately starting the policy with something of an antagonistic nature. “Internet use policy” is a more neutral heading that does not necessarily suggest rules and regulations, rather, it is a statement describing what the library ICT facilities can offer. “Acceptable use policy” is a widely-used term however and as such it may be more familiar to library users, therefore the library service may feel more comfortable using that as a title for their policy.

7.3 Authorship

An AUP created by one group, such as CILIP, would mean it could be well-informed – pulling together legal, ethical, and technical experts – and would mean no further effort is necessary on the part of the library team of each individual PLA. Sturges (2002) notes that an AUP created in-house allows for the policy to be truly owned by the individual PLAs and will fit the organisation better than one that is made by compiling elements from other AUPs found online. A generic policy could also fall into the trap of not being individual enough for each institution. However, a model policy could be helpful in that it lays out the groundwork

which each PLA can fit their own policy into. It would also mean that the library ICT service is uniform across institutions, and patrons would not be provided or denied services just because they happen to live in a particular area in the UK.

7.4 Design

A well-written AUP can be backed up by a visually stimulating presentation. Whilst some of the AUPs from this study had colourful borders, headings, and writing, most were simply a wall of black text, sometimes without headings or any real sense of structure. Many of the AUPs lacked colour or decoration, and were simply designed as blocks of text for the user to read through. Whilst words are obviously one of the most straightforward ways to disseminate information, perhaps designing the documents in a more colourful and aesthetic way, with accompanying illustrations, charts, or even a video or animation would lead to patrons paying more attention to this important document, and help to connect them to the text more, allowing for a more deeper understanding of the policy and the ideas behind it. Using more colourful formatting, with illustrations, images, or a video could be a more effective way to communicate the AUP. Interactive elements could also help to encourage users, especially those at a lower literacy level to fully comprehend the document, and engage with the material in a deeper way. Although the model policy is given here in a basic form, it would be possible to supplement it with interactive elements, and colourful formatting.

7.5 Model policy

The AUP document must be designed in such a way that it is appropriate for a wide audience – the library service has to cater to the community, young, old, with or without further education. As well as being easily understood, it must also draw the attention of the user. It has been acknowledged that AUP documents are not necessarily given the appropriate amount of attention from both staff and users alike. As noted by previous studies, there is both a lack of awareness and an apathy towards the AUP (Höne and Eloff, 2002; Laughton, 2008; McMenemy, 2008; Poulter et al., 2009; Doherty et al., 2011; Spacey et al., 2014). Having a document that is easily read is paramount to this process.

The policy took a number of redrafts. The first version scored at a high level of difficulty when put through the readability testing website. The initial version scored as follows:

- Flesch Reading Ease: 56.3
- SMOG Grade: 12.1
- Gunning Fog Index: 11.6
- Coleman-Liau Index: 9.8

The version provided as Appendix 2 (the sixth version) scored as follows:

- Flesch Reading Ease: 66.7
- SMOG Grade: 9.4
- Gunning Fog Index: 8.0
- Coleman-Liau Index: 8.0

The initial version used too many long words, passive voicing, and complex sentences. Paragraphs such as:

- ***It should be noted that filtering is not fool proof. Guardians should make sure to supervise their child's use of the facilities. If you find that filtering has blocked a website that you wish to access or has let through a website that you think should be blocked, please tell us by email, asking a member of staff, filling out a webform or writing a note in the comments box and we will look into this for you. All suggestions will be treated with the strictest confidence.***

Was changed to:

- ***Please note that filtering is not fool proof. Filtering can block websites or let through websites by mistake. Adults should make sure to supervise their child's use of the Internet. If you find a filtering error, please tell our staff. You can also email, webform, or post a note in the comments box. We treat all suggestions with the strictest confidence.***

The second paragraph uses the active voice instead of the passive at the start, and breaks the longer sentences up. The first paragraph used 87 words whilst the second only used 61. Readability testing allows for simplifying more difficult pieces of text, and thus will make it more likely for the patron to read it.

A breakdown of what the policy should contain now follows. The model policy appears in full as Appendix 2.

7.6 Policy breakdown

7.6.1 Welcome section

Of the 205 AUPs analysed, 63 had no opening statement, instead launching straight into the terms and conditions of service. It is important, as noted by Sturges, that an AUP should talk to those it has been created for, and not just be "put together for its own sake" (Sturges, 2002: 108). An introductory section, or a welcoming statement is an important part of this process. A document that begins in a flat, clinical fashion will fast lose readership. One that starts off welcoming the patron will help to engage those that might otherwise be discouraged from reading policy documents. It should be explained why the service is there. Aims and objectives is the first essential feature on Sturges' list, and the intentions of the service are an important part of comprising an AUP (Scott and Voss, 1994; Palgi, 1996; Kelehear, 2005; Pautz, 2013). Following guidelines from the ALA's *Libraries and the Internet Toolkit* and also CILIP's *Ethical Principles* document, the AUP should also encourage access and show its commitment to access for all users. The opening statement speaks to what the service provides, as well as ensuring inclusivity through the use of access requirements, as well as establishing how important the service is within the community. It was found by the researcher that the AUPs that contained a welcoming statement, encouraging the use of the facilities was a more pleasant experience for the reader, as those that left this section out tended to read very dry, as a list of rules, rather than a communication to the patron.

7.6.2 Eligibility

Stating eligibility, such as if the service is provided for all or on a members-only basis, along with guidelines regarding children's usage is the second essential feature on Sturges' list. 81 of the 205 AUPs analysed gave information on this, with 57 describing eligibility in a full way. It was important to establish who can use the service, in terms of visitors, members, and children. An important part of the AUP is establishing conditions of access (McMenemy, 2014) of which, setting out time allowance is one (ALA, 2007b). Usage should be encouraged, so allowing users to extend access if no-one is waiting both encourages access and makes sure there is fair use for all, and helps to establish CILIP's ethical principle of equitable treatment and best provision.

7.6.3 Scope of service and filtering information

It is important to state what the limits of the service are, and whether this includes personal use (Sturges, 2002; McMenemy, 2009). As noted by a number of guidelines, explanations should be clear, avoiding too much jargon (e.g. Scott and Voss, 1994; Palgi, 1996; Höne and Eloff, 2002; Sturges, 2002; ALA, 2007b; Pautz, 2013). One of the key findings from the MAIPLE Project was the lack of clarity regarding the use of filtering, noting that half of those users who were interviewed were found to be unaware of its usage (Spacey et al., 2014: iv). Thus, the use of filtering was explained in as clear and concise a way as possible. It was important for the user to understand what filtering is and why it is there; concern for the public good being a key ethical principle from CILIP. It was also important to ensure users knew what to do in the case of the filtering software being in error. Encouraging information access is a key part of any library service and is one of CILIP's ethical principles. Also, the MAIPLE Project and McMenemy's unobtrusive testing study both found filtering unblocking processes to be inconsistent (McMenemy, 2008; Spacey et al., 2014) and half of the interviewees for the MAIPLE Project stated discomfort at the prospect of asking staff members to unblock websites that had been filtered "however legitimate the site may be" (Spacey et al., 2014: iv). As well as this, the findings from this study suggested that filtering information, particularly unblocking, is not well communicated to public library patrons.

Explaining what to do when filtering software makes an error, and providing an anonymous way of doing so, was seen to be an important part of explaining the use of filtering.

7.6.4 Misuse

Defining what constitutes as misuse and illegal use is a key part of any AUP (Scott and Voss, 1994; Sturges, 2002; Kelehear, 2005; ALA, 2007b; Laughton, 2008). The findings from Gallagher et al., (2015) and this study helped to inform the tone of this section; care was taken to not be too authoritarian. Again, the mention of legislation was coupled with explanations so as not to pass the burden of understanding undefined laws onto the patron (McMenemy, 2014). Mentioning unacceptable use in relation to others was also key to ensure the library is seen as a communal space, that users should be aware of others, and to remain committed to the public good. It was important to encourage freedom of expression whilst reminding the patron that the space they are in is a public one.

7.6.5 Service Commitments

It's important that users are clear regarding the library service and its responsibilities regarding information found on the Internet. The AUP must protect the institution in regards to any possible liabilities (Kelehear 2005; Laughton, 2008). Again, privacy is an important commitment from the library service, as users need to be able to trust that their information will be handled correctly.

7.6.6 User Commitments

It is important for the patron to understand their responsibilities in relation to the library service and to other users. The AUP must detail what will happen in the event of a patron misusing the service, such as any disciplinary procedures (Sturges, 2002). Again, transparency was key here, so as to inform patrons of their rights, and to make sure they understand the process of possible suspension from the service.

7.7 Conclusion

This chapter has presented the outline of a model policy, which has been informed both by the literature review and also the findings of this study. The full model policy appears in Appendix 2. The next chapter will give a concluding summary, with the response to the

research questions contributions of this research, along with final thoughts and recommendations. Possible future areas of research will also be outlined here.

8 Conclusion

8.1 Introduction

This study aimed to assess public library AUPs of the UK, to find out whether they demonstrate characteristics of the panoptic principle, along with how they frame access to ICT facilities, including surveillance and filtering, freedom of expression, and commitment to ethical principles, and how they balance the caring and controlling aspects of public access.

AUP research is relatively rare, and this research has contributed to the lack of material on this subject. The use of readability testing, and FOI requests are also relatively under-used in library and information science. 205 of the possible 206 AUPs from UK public libraries were collected and analysed. It was found that the AUPs in the UK are very varied, too difficult to be read easily, are representative of CILIP's ethical principles, but also have aspects of the panoptic principle, along with heavily referencing compliance and misuse rather than elements such as aims and objectives. It is difficult to maintain a balance between protecting the library service's user base whilst also allowing for individual privacy and freedom of expression.

ICT access in the public library needs to be managed in some format: there are stakeholders to think of, such as the PLA's citizens and the individual library's local community, local councils, government and governing bodies, and ultimately the wider taxpayers who help to fund the public library. These stakeholders will expect the access to be managed in some way. Caregivers will expect children's access to be safe and protected from harm, the taxpayer will be wary of the library being used for illegal purposes. In the same way that access to reading materials is managed – signage and staff are there to provide guidance allowing patrons to make the most out of their library service. Access that is managed well can provide a patron with an effective service that they may have been too apprehensive to use on their own at home and this can be combined with a well-written AUP that can help to reassure patrons and inform them of what they can expect from their public library service.

What follows is an overview of this study's conclusions, and the response to the research questions as initially outlined in the methods chapter, along with the study's contribution to knowledge. Lastly there will be some final recommendations along with potential areas for further research.

8.2 Conclusions

This study sought to answer these research questions:

- RQ1 In what ways does the public library AUP document reflect the panoptic principle?
- RQ2 How does the public library AUP encourage and discourage access to information and freedom of expression through surveillance, filtering, and commitment to ethical principles?
- RQ3 How effectively does the AUP balance the care and control elements of public access?

8.2.1 RQ1

The AUPs reflect the panoptic principle by overly relying on controlling ways of describing surveillance. With over half of the AUPs featuring the monitoring control node, and surveillance being used to ensure that patrons were using the facilities in an appropriate way – surveillance is used to ensure compliance from the patrons, and in a disciplinary way, as described by Foucault. This is also reflected in the references to the panoptic gaze throughout the AUPs. The use of random checking, messages appearing onscreen to remind users that they are being observed, and the use of uncertainty – surveillance may be used – all suggest panopticism. Patrons were also sorted into legitimate and non-legitimate users, again, this notion of discipline being a key aspect of panopticism. The reliance on authoritarian language, authoritarian displays of power, and discipline, with lack of an appeals procedure also suggest panopticism is relevant in the public library AUP.

Despite this, there was also aspects of caring and protective surveillance, although this was by a far fewer number of the AUPs, with monitoring neutral being ahead of monitoring care.

The adherence to CILIP's ethical principles also go against the disciplinary nature of panopticism, suggesting that although panopticism is reflected in the AUPs, there is also a focus on care. Stating that the library service cares for its users and wishes to commit to access to information is undermined by the disciplinary use of surveillance.

8.2.2 RQ2

The use of surveillance, in particular the use of controlling surveillance may have a discouraging effect on library patrons' ability to exercise freedom of expression and access to information. Such heavy-handed use of surveillance, alongside the opaque nature regarding the usage of filtering software may lead patrons to self-censoring, thus having a chilling effect. One of the key aspects of an AUP is demonstrating how the service can be used, and what the public library service hopes to offer its patrons.

The AUPs overall represented CILIP's ethical principles fairly well, especially those pertaining to encourage access such as promoting equal rights and commitment to access to information. However due to a sizeable chunk of the AUPs only taking a minimal approach to describing the service, this was varied.

The varied nature of the AUPs means that whilst some patrons have a detailed account of what is available from their public library service, along with a thorough description of filtering software and what to do if it does not function correctly, and an encouraging welcoming statement describing the facilities on offer, some patrons are faced with a document that has little information to offer in terms of their access rights, instead opting to set out a list of rules and regulations. The lack of a proper aims and objectives section in many of the AUPs, or with some having no opening preamble at all, does not encourage patrons to have full use of the facilities.

The overall difficulty of the AUPs in terms of readability also suggests that access is discouraged. The AUP, as an important document between the patron and the public library institution, has the power to both promote and hinder information access. As such, the document should be accessible by all users who wish to use the ICT facilities of the public

library. If the AUP is not easily read by the patrons that the library serves, it is not a fair document for the patron to read and be bound by, and it does not adequately cover the library in the case of inappropriate activity. An AUP that is difficult to understand does not encourage the patron to access information either: a difficult to follow, vague, or confusing AUP can actively hinder a patron's attempt to access information, which goes directly against the purpose the public library serves. If the patron does not understand all that is being offered to them in the AUP document, they cannot make effective use of the facilities, which hinders the service and their information access. In order for an AUP to inform the library patrons about access and to properly promote freedom of expression, the document has to be both informative, and readable. If patrons are not properly informed about the services they are accessing, then the library service is on dubious ground regarding the contractual status and protection that the document provides. It also means that the library service is not committing to some of CILIP's fundamental ethical principles, such as Principle 1, "Concern for the public good in all professional matters, including respect for diversity within society, and the promoting of equal opportunities and human rights". Promoting equal opportunities relies on everyone being properly informed. It also goes against Principle 3: "Commitment to the defence, and the advancement, of access to information, ideas and works of the imagination." An AUP that is not properly informative and easily comprehended does not lend itself to the advancement of access to information.

8.2.3 RQ3

The public library AUP is varied. Whilst it attempted to encourage access through CILIP's ethical principles and caring uses of surveillance, the use of controlling surveillance, the difficulty of the documents, and the lack of information with regards to filtering means that the AUPs of public libraries in the UK are controlling rather than caring. Whilst it is important to inform users as to what constitutes inappropriate behaviour in a public library setting, and to outline the response of the library if someone starts to exhibit these behaviours, care should be taken by the PLA as to what sort of language is used when informing patrons about this. The use of words such as "obey" are perhaps overly authoritarian in tone. In this

study, Compliance was one of the most heavily referenced nodes, and monitoring control was present more than monitoring care. The library service must ensure its services are not going to be used for criminal or inappropriate activities – particularly in a public environment with children and vulnerable individuals present – however, it must also ensure that users are not put off by heavy-handed language. It is clearly difficult to balance aspects of care and control and there is a tension between protecting the community, making sure the library service is safe from illegal activity, and becoming overly restrictive on individual privacy and freedom, along with sounding overly authoritarian in tone.

The library must balance providing safe, reliable, ICT facilities, encouraging their usage, whilst also making sure that these services do not get misused. There is a tension in the AUPs, between caring for the patrons, their access to information, and their safety, and making sure that guidelines regarding misuse and how the library service responds to such misuse is communicated clearly. CILIP's ethical principle of "Concern for public good, respecting diversity and promoting equal opportunity and human rights" is the one of the most well-represented themes. However, there is also a heavy emphasis on misuse and sanctions for any inappropriate behaviour. Only three of the AUPs made no mention of illegal or inappropriate usage, and 196 of the AUPs listed some sort of banning procedure or sanctions being handed out in the event of inappropriate activities or use of the facilities. Whilst it is important to outline such usage – with those AUPs not referencing such usage becoming open to possible misuse with no defence – the references to banning and misuse outnumber references of other elements of the AUP, such as CILIP's third ethical principle regarding information access, and the aims and objectives element from Sturges' recommendations for an AUP. Describing misuse in the context of protection and care only occurred in 129 of the AUPs. One of the most referenced of the nodes was compliance, with 754 references overall, in all 205 of the sources. Lyon's spectrum of care and control (1994; 2001) was in evidence in the AUPs: the tension between using surveillance to ensure that users behave appropriately, monitoring for misuse and ensuring compliance, alongside

using surveillance as a way to improve the service and for the safety of its patrons. As Monahan (2011) notes, sometimes surveillance lies in the centre, where care and control meet. The analysis of the AUPs showed the difficult balance the library service has to tread between protecting the safety of its patrons, ensuring privacy, and allowing individuals to enact their information rights.

8.3 Contributions to knowledge

- This research has contributed a new understanding of access management in public libraries. This research has added new insight by studying the content of AUPs, an integral part of managing Internet access in public libraries. This research contributes to the limited research that exists on public library AUPs in the UK. Previous research has incorporated surveys, FOI requests, and discourse analysis, but not from the entirety of the UK. This research analysed AUPs from 205 PLAs in the UK, a return rate of 99.5%. This research highlights the variable nature of a document that is supposed to function as an interface between the library patron and the ICT services they are using. That the service is not carried out consistently across the UK should be a cause of concern for practitioners and policymakers alike.

- This research has contributed a new understanding of filtering practices as evidenced in AUP documentations across UK public libraries. Building on studies such as the MAIPLE project (Spacey et al., 2014) and Gallagher et al.'s study (2015), this research contributes an expanded understanding of how many PLAs use filtering software, offer information on unblocking, and how it is framed.

- There has also been a new understanding gained regarding access management in UK public libraries and how power, surveillance and information ethics are communicated to library patrons. Previous research has been used to study AUPs on a smaller scale (e.g. Gallagher et al., 2015). Alongside this, the research has

contributed to a further understanding of ethical principles regarding information access, privacy, and freedom of expression, and how they are treated and expressed in the public library.

- This research has also contributed to the lack of research on panopticism in public libraries in the UK, and has contributed a new understanding of panopticism and disciplinary surveillance in public institutions such as libraries. Prior to this research, panopticism research has mostly been restricted to the analysis of Victorian libraries and small-scale studies (Hewitt, 2000; Black 2001; Black 2005; Gallagher et al., 2015).

- This study provides a readability analysis of 99.5% of the AUPs in the UK, and has found that a large number of public library AUPs are not easily comprehended for the general public. This research has contributed to the lack of readability testing in the information science sector. Readability testing is a useful method of analysing the comprehensibility of text, but it is not widely practised outside of medical and legal policies, and other medical documentation such as consent forms and health information websites. This study has used readability to analyse policies and also in the creation of a policy that will be better comprehended by readers.

- This research has also contributed to knowledge by providing a possible model policy that can be used by public libraries. Currently, each PLA has to create their own, custom AUP. This means a lack of consistency across the service leading to a "postcode lottery" (McMenemy, 2014: 11) for patrons in terms of what type of service they will have access to. The model created has been drawn from best practice in the literature, as well as previous studies into access management in UK public libraries. It has been tested for readability and redrafted accordingly to ensure comprehension

will be optimal. By dissemination through a Creative Commons licence, the model policy can be freely used and distributed by others.

8.4 Recommendations

8.4.1 Authorship and a national AUP

The AUPs were written by a variety of personnel in the library service itself, and the greater staff of the PLA in general. It makes no real sense for each PLA to have a separate AUP. The differences between each document, as witnessed by this study, indicate that access is not uniform for public library visitors across the UK. What is permitted in one institution will not be permitted in another, with access restrictions and costs differing between PLAs. A public library service should not change across different parts of the country. As well as being unfair for library patrons, it seems to be a waste of time for each PLA to have to take the time to construct their own AUP. That each PLA uses different parts of each council's service also adds to the confusion, and documents are produced that are informed by legal teams, IT departments, and disparate council members. An AUP in one PLA may be legally informed and more able to protect the institution, whilst an AUP in another PLA may have no legal input whatsoever. A national AUP could be informed by various entities meaning a well-rounded, well-informed, legal and ethically sound document that library staff can be uniformly trained on and be confident in. For an AUP to have enough information yet also make sense, whilst also covering the library service and the authority itself, it might be wise to call on a number of consultants to ensure the AUP is up to a high standard. Library staff themselves could inform its creation, for they are on the front-line and deal with library users every day. IT would be helpful to ensure the technical components of the document are outlined clearly. Having IT staff to create the document alone could serve to make the document too technical and lack crucial elements such as CILIP's ethical principles. A member of the legal team can make sure the library service is covered by the document whilst also ensuring enough legal information is being provided for patrons to follow. Not every PLA has the time or the resources to pull together such a team, thus a single AUP for

all PLAs would mean less of a drain on resources, better coverage for the library services, and equal access conditions across authorities. If staff in individual PLAs were not directly involved, training would be crucial to ensure all staff are informed of the AUP, and its contents. A national AUP, complete with strong training in its deployment, would establish a library service culture that is fully informed and confident about their AUP.

Sturges (2002) notes that a well-written AUP takes time to craft, and will need regular updating as technology, legislation, and the library environment change. Having one team responsible for constructing the AUP will cut down on resources required and also ensures that the AUPs are maintained and up-to-date. Some of the AUPs analysed in this study had not been updated for a number of years.

The AUP should be written in a way that is easy to understand. Passing the policy through readability tests would be an effective way to ensure the document is suitable for all those reading it. As mentioned before, some of the AUPs were quite drab in presentation. The researcher found AUPs that were a block of text more boring and laborious to read than those featuring colourful borders and headings. An AUP supplemented with visuals may hold the reader's attention better. Again, on an individual business this could be a time-consuming and potentially expensive task, however, if there was a single, national AUP, this would need to be created only once, instead of 206 times.

It is important that the AUP, when deployed, has the backing of the frontline members of the library service. The AUP should not be seen as a screen to be bypassed, but as an integral part of accessing information via the library service's IT facilities. If the AUP is written in a way that is both informative and robust, the library staff will know they can depend on it. An AUP that has backing from those that will be interacting with it on a daily basis – the frontline staff of the library service – will be more robust and will be a document that staff can have faith in.

8.4.2 Filtering

It is a concern that only some of the AUPs state that filtering is or is not in use. Other studies, as mentioned in the access management literature review chapter, have found widespread use of filtering software. The authorities that do not use filtering software explicitly say so, so it may be inferred that the number of AUPs that do not mention it are using filtering software but are simply failing to communicate this in the AUP. If filtering is to be used, it should be used in such a way that is clear to the user, along with a system in place for access to information that has been incorrectly blocked. It takes only a few lines to outline the filtering policy of the authority; a small paragraph or two, is all that is needed to define the authority's filtering policy. Filtering software may be necessary for managing public access – the public library environment should be a safe space for visitors to find information, and, as with the selection process, the librarian does not simply fill the shelves with every book imaginable so, it can be argued, Internet access should be the same. However, it is important that patrons are informed of the usage of such software, and patrons should be made aware that filtering is in operation on their machines.

The AUP should also contain information on the efficacy of filtering software and what the patron should do if the filtering software does not work correctly. If filters are to be used, there should be a simple, preferably anonymous, solution to unblocking websites that patrons feel are legitimate. Patrons should feel comfortable with the process of getting a website unblocked: patrons are less likely to request unblocking if the website in question discusses delicate matters such as information regarding one's health. An anonymous request form accessed online, or a physical drop-in box situated in the library would be ideal solutions. Of course, the option should be there to simply ask a member of staff about unblocking or blocking content, but not every library user will have the confidence to do so.

8.4.3 Levelled filtering

A tiered system of filtering websites could also be a good solution. Sexual health or murder mystery websites may not be appropriate for those who are very young, however young

adults and older members of the library service should be able to choose whether they wish to visit those websites or not. The walled-garden approach by some library services could be an effective way of making sure younger children have access in a supported, safe environment. A nuanced approach to filtering means that vulnerable users will be protected, whilst information will not be denied to those who may seek it.

8.4.4 Surveillance

If monitoring is being used in the public library, it should be communicated to the patron in a helpful way, so as to promote care and safety. In an attempt to protect patrons – particularly those in vulnerable groups such as young children – monitoring measures such as filtering and surveillance of patrons which should be used as caring apparatus can easily be framed in such a way as to become controlling apparatus. What is meant to be used to protect or care for patrons can actually become inhibitive for a patron's use of the ICT facilities. If surveillance is being carried out, it should be limited, suitable for the situation, and communicated in an appropriate way, avoiding authoritarian language.

8.5 Further research

It would be informative to find out how other libraries – those in the education sector for example, and those in other countries – compare to the results found here. Also, research into other types of institutions are relatively rare – there has been some investigation into AUPs in the healthcare sector and the business sector, but not to a great extent. For such an important document – for both the institution and the computer user – it is surprising that more research has not been done on this topic.

This research was concerned with the AUP documents themselves, and they communicated various aspects of the library service and practice within. Future research could go towards investigating how the AUP aligns with actual practice in libraries.

Whilst informative, the qualitative content analysis only captured certain aspects of the documents. While reading through the AUPs, the researcher noted the very varied

information regarding children's access. Although access by children tended to be encouraged in the AUPs, age limits and parental consent varied between AUPs, with no clear guiding principle as to when children need supervised access and when they are old enough to surf the Internet without an adult present. A similar study using content analysis could capture the different age ranges alongside analysis to find out how children's access is discussed in the AUPs. These could be compared with AUPs in the educational sector to get a clearer picture of children's access to ICT facilities in the UK.

Likewise, elements such as charging for Internet access and printing privileges could be looked into further – there was variability between AUPs, with some charging a nominal fee for Internet access, or yearly subscription, with others providing access with no charge. Considering the public library's important role as information and Internet provider – particularly for those who have no access to the Internet at home – it is perhaps a concern that some authorities charge for Internet access and some do not.

8.6 Final thoughts

By using readability analysis and qualitative content analysis this study aimed to investigate the content of AUPs in UK public libraries. The AUPs were analysed to find out if they contained elements of the panoptic metaphor, as established by Michel Foucault. It was found through the use of surveillance, and disciplinary mechanisms that a number of AUPs used for public libraries do contain elements of panopticism. Alongside this the AUPs were found to both promote and prohibit access to information. By being difficult to read, and written by a variety of different groups, the AUPs were inconsistent between PLAs. For some patrons, the complex nature of the documents could render them difficult to understand and thus be prohibitive to information access. The AUPs promoted access to information through the use of CILIP's ethical principles. In particular, children's access was widely encouraged. The use of overly negative language, and certain controlling aspects of the AUPs can prohibit rather than promote access. The use of filtering was widespread, and the lack of explanation regarding its use could prohibit access to information. For filtering to work, it is

recommended that there be further explanation in the AUPs, and for frontline staff to be able to unblock websites. Having different levels of filtering, including specific PCs for children-only, or PCs that are completely unfiltered, could allow for patrons to access information unfettered if they wish.

This research has provided a new perspective on Internet access management in public libraries, with a thorough investigation of AUPs, across the whole of the UK. It has provided a possible model AUP that has been tested using readability software, making what is an often complex document into one that is hopefully more easily comprehended for all library visitors.

9 References

ACETO, G. & PESCAPÉ, A. 2015. Internet Censorship detection: A survey. *Computer Networks*. 83, pp. 381-421.

AGARWAL, N., CHAUDHARI, A., HANSBERRY, D. R., TOMEI, K. L. & PRESTIGIACOMO, C. J. 2013. A comparative analysis of neurosurgical online education materials to assess patient comprehension. *Journal of Clinical Neuroscience,* 20(10)**,** pp.1357-1361.

AINLEY, R. 1998. Watching the detectors: control and the Panopticon. In: R. AINLEY. ed. *New Frontiers of Space, Bodies and Gender.* London: Routledge, pp.88-100.

ALA. 2007a. *Questions and Answers on Privacy and Confidentiality*. [Online]. Available: <http://www.ala.org/advocacy/privacy/FAQ> [Accessed: 05/04/2019]

ALA. 2007b. *Libraries and the Internet Toolkit.* [Online]. Available: <http://www.ala.org/advocacy/intfreedom/iftoolkits/litoolkit/internetusepolicies> [Accessed: 05/03/2017]

ALA. 2008a. *Code of Ethics of the American Library Association*. [Online]. Available: <http://www.ala.org/advocacy/proethics/codeofethics/codeethics> [Accessed: 20/10/2015]

ALA. 2008b. *Privacy*. [Online]. Available: <http://www.ala.org/advocacy/privacy> [Accessed: 05/04/2015]

ALA. 2012. *Libraries and the Internet Toolkit*. [Online]. Available: <http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/intfreedom/iftoolkits/litoolkit/2012internettoolkit.pdf> [Accessed: 24/02/2017].

ALA. 2015. *Internet Filtering*. [Online]. Available: < http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/internet-filtering> [Accessed: 25/03/2019]

ALEXANDER, L. A. & HORTON, P. 1983. The impossibility of a free speech principle. (Symposium: freedom of expression: theoretical perspectives). *Northwestern University Law Review,* 78(5)**,** pp.1319-1357.

ALMOND, P. 2008. Investigating health and safety regulation: Finding room for small-scale projects. *Journal of Law and Society,* 35(1)**,** pp.108-125.

ALTHEIDE, D.L. 1996. *Qualitative Media Analysis*. Thousand Oaks, CA.: Sage.

ANDERSON, D. 2015. A question of trust: Report of the investigatory powers review. [Online] Available: < https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review> [Accessed: 26/04/2019]

ANDREJEVIC, M. 2002. The kinder, gentler gaze of big brother. *New Media & Society,* 4(2)**,** pp.251-270.

ANDREJEVIC, M. (2011) Surveillance and alienation in the online economy. *Surveillance & Society*, 8(3), pp.278-287.

ANDRZEJEWSKI, A. V. 2008. *Building Power: Architecture and Surveillance in Victorian America*. Knoxville: University of Tennessee Press.

AULD, H. & KRANICH, N. 2005. Do Internet filters infringe upon access to material in libraries? *Public Libraries,* 44(4)**,** pp.196-204.

BADARUDEEN, S. & SABHARWAL, S. 2010. Assessing readability of patient education materials: current role in Orthopaedics. *Clinical Orthopaedics and Related Research,* 468(10)**,** pp.2572-2580.

BAKER, C. E. 2011. Autonomy and free speech. *Constitutional Commentary*, 27(2), pp.251-282.

BAKIR, V. 2015. “Veillant panoptic assemblage”: Mutual watching and resistance to mass surveillance after Snowden. *Media and Communication*, 3(3), pp.12-25.

BARENDT, E. M. 2007. *Freedom of Speech.* Oxford: Oxford University Press.

BARNARD-WILLS, D. & WELLS, H. 2012. Surveillance, technology and the everyday. *Criminology and Criminal Justice,* 12(3)**,** pp.227-237.

BARNARD-WILLS, D. 2011. UK news media discourses on surveillance. *The Sociological Quarterly,* 52(4)**,** pp.548-567.

BBC. 2015. *CCTV: Too Many Cameras Useless, Warns Surveillance Watchdog Tony Porter*. [Online]. Available: < http://www.bbc.co.uk/news/uk-30978995> [Accessed: 20/10/2015]

BECTA. 2009. *AUPs in Context: Establishing Safe and Responsible Online Behaviours* [Online]. Available: <http://www.wisekids.org.uk/BECTA%20Publications/aups_context_online_behaviours.pdf> [Accessed 08/02/17].

BENTHAM, J. & BOWRING, J. 1843. *The Works of Jeremy Bentham*. London: W. Tait. [Online]. Available: <https://oll.libertyfund.org/titles/1920> [Accessed: 10/05/17].

BENTHAM, J. & QUINN, M. 2001. *Writings On The Poor Laws.* Oxford: Oxford University Press. Original published 1843.

BERELSON, B. 1952. *Content Analysis in Communication Research*. New York: Free Press.

BEST, J., MUZAFFAR, J. & MITCHELL-INNES, A. 2015. Quality of information available via the internet for patients with head and neck cancer: are we improving? *European Archives of Oto-Rhino-Laryngology,* 272(11)**,** pp.3499-3505.

BEST, R. H. 2009. Panopticism and the use of "the other" in To Kill A Mockingbird. *The Mississippi Quarterly,* 62(3/4)**,** pp.541-552.

BEVIR, M. 1999. Foucault, power, and institutions. *Political Studies,* 47(2)**,** pp.345-359.

BIRKINSHAW, P. 2001. *Freedom of Information: The Law, The Practice, The Ideal.* London: Butterworths.

BLACK, A. 2001. The Victorian information society: surveillance, bureaucracy, and public librarianship in 19th-century Britain. *The Information Society,* 17(1), pp.63-80.

BLACK, A. 2005. The library as clinic: a Foucauldian interpretation of British public library attitudes to social and physical disease, ca. 1850-1950. *Libraries & Culture,* 40(3)**,** pp.416-434.

BLACKFORD, H. 2004. Playground panopticism: ring-around-the-children, a pocketful of women. *Childhood,* 11(2)**,** pp.227-249.

BLAND, A. 2014. *The rise of GoPro: why wearable cameras make us film everything. The Guardian.* 4 October. [Online]. Available: < http://www.theguardian.com/technology/2014/oct/04/rise-of-gopro-wearable-cameras> [Accessed: 20/10/2015]

BLOSS, W. 2007. Escalating US police surveillance after 9/11: An examination of causes and effects. *Surveillance & Society*, 4(3), pp.208-228.

BLOUSTEIN, E. J. 1964. Privacy as an aspect of human dignity: an answer to Dean Prosser. *New York University Law Review,* 39(6)**,** pp.962-1007.

BLUMAN, E. M., FOLEY, R. P. & CHIODO, C. P. 2009. Readability of the Patient Education section of the AOFAS website. *Foot & Ankle International,* 30(4)**,** pp.287-291.

BOYNE, R. 2000. Post-panopticism. *Economy and Society,* 29(2)**,** pp.285-307.

BRADBURN, N., SUDMAN, S., & WANSINK, B. 1982. *Asking Questions: The Definitive Guide to Questionnaire Design: For Market Research, Political Polls, and Social and Health Questionnaires*. San Francisco: Jossey-Bass.

BRANCO, P. 2010. On prisons and theatres: Santo Stefano and San Carlo. *Law Text Culture,* 14**,** pp.277-285.

BRIGO, F., OTTE, W. M., IGWE, S. C., TEZZON, F. & NARDONE, R. 2015. Clearly written, easily comprehended? The readability of websites providing information on epilepsy. *Epilepsy & Behavior,* 44**,** pp.35-39.

BRINGER, J. D., JOHNSTON, L. H. & BRACKENRIDGE, C. H. 2004. Maximizing transparency in a doctoral thesis1: the complexities of writing about the use of QSR*NVIVO within a Grounded Theory study. *Qualitative Research,* 4(2)**,** pp.247-265.

BRISON, S. J. 1998. The autonomy defense of free speech. *Ethics,* 108(2)**,** pp.312-339.

BRITAIN, T. *Archive Journeys: Tate History* [Online]. Available: <http://www2.tate.org.uk/archivejourneys/historyhtml/bld_brit_site.htm> [Accessed 20/10/2015].

BROPHY, P. 2003. *The People's Network: a turning point for public libraries: first findings* [Online]. Resource: The Council for Museums, Archives and Libraries. Available: <http://www.slainte.org.uk/SLIC/peoplesnet/pn_a_turning_point_2002.pdf> [Accessed 15/3/2017].

BROWN, G. T. & MCMENEMY, D. 2013. The implementation of internet filtering in Scottish public libraries. *Aslib Proceedings,* 65(2), pp.182-202

BROWN, K. J. 2009. COUNTERBLAST: Freedom of information as a research tool: realising its potential. *The Howard Journal of Criminal Justice,* 48(1)**,** pp.88-91.

BRYMAN, A. 2012. *Social Research Methods.* 4th Edition. Oxford: Oxford University Press.

BRYMAN, A. 2016. *Social Research Methods.* 5th Edition. Oxford: Oxford University Press.

BUDD, J. 2006. Discourse Analysis and the study of communication in LIS. *Library Trends,* 55(1)**,** pp.65-82.

CAMPBELL, D. GRANT & COWAN, SCOTT R. (2016). The paradox of privacy: Revisiting a core library value in an age of big data and linked data. *Library Trends*, 64(3), pp.492-511.

CANTORE, S. & PASSMORE, J. 2012. *Top Business Psychology Models: 50 Transforming Ideas for Leaders, Consultants and Coaches.* London: Kogan Page.

CAPUTO, V. 2007. She's from a good family' performing childhood and motherhood in a Canadian private school setting. *Childhood,* 14(2)**,** pp.173-192.

CHAABANE, A., KAAFAR, M.A. & BORELI, R. 2012. Big friend is watching you: analyzing online social networks tracking capabilities. *Proceedings of the 2012 ACM workshop on Workshop on online social networks (WOSN '12)*. ACM, New York, NY, USA, pp.7-12.

CHAABANE, A., CHEN, T., CUNCHE, M., DE CRISTOFARO, E., FRIEDMAN, A. & KAAFAR, M.A. 2014. Censorship in the wild: Analyzing Internet filtering in Syria.

Proceedings of the 2014 Conference on Internet Measurement Conference pp. 285-298. ACM.

CHEN, J. V., CHEN, C. C. & YANG, H.-H. 2008. An empirical evaluation of key factors contributing to internet abuse in the workplace. *Industrial Management & Data Systems,* 108(1)**,** pp.87-106.

CILIP 2015. *Libraries and Information Services in the United Kingdom and the Republic of Ireland 2015.* London: Facet.

CILIP. 2011. *User Privacy in Libraries: Guidelines for the Reflective Practitioner* [Online]. Available: <https://www.cilip.org.uk/sites/default/files/documents/Privacy_June_AW.pdf> [Accessed 01/03/2017].

CILIP. 2012. *A Changing Landscape: A Survey of Public Library Authorities 2012-13* [Online]. Available: <http://www.cilip.org.uk/cilip/advocacy-awards-and-projects/advocacy-and-campaigns/public-libraries/briefings-and-resources>. [Accessed 25/11/2016].

CILIP. 2013. *Ethical Principles*. [Online]. Available: <http://www.cilip.org.uk/cilip/about/ethics/ethical-principles> [Accessed: 20/10/2015]

COFFIN, C. 2001. Theoretical approaches to written language: A TESOL perspective. In: B.A. COFFIN. ed. *Analysing English in a Global Context: A Reader.* London: Routledge.

COHEN, J. E. 2013. What privacy is for. *Harvard Law Review,* 126(7)**,** pp.1904-1933.

COLEMAN, M. & LIAU, T. L. 1975. A computer readability formula designed for machine scoring. *Journal of Applied Psychology,* 60(2)**,** pp.283-284.

COLOMBAT, A. P. 1991. A thousand trails to work with Deleuze. *SubStance,* 20(3)**,** pp.10-23.

COOKE, L. 2006. Do we want a perfectly filtered world? (Guest editorial). *Library Student Journal,* 2. [Online]. Available:

<htttp://www.librarystudentjournal.org/index.php/lsj/article/view/21/162> [Accessed 20/10/2016]

COOKE, L., SPACEY, R., CREASER, C. & MUIR, A. 2014. "You don't come to the library to look at porn and stuff like that": Filtering software in public libraries. *Library and Information Research,* 38(117)**,** pp.5-19.

CORCORAN, N. & AHMAD, F. 2016. The readability and suitability of sexual health promotion leaflets. *Patient Education and Counseling,* 99(2)**,** pp.284-286.

COTTRELL, J. R. 1999. Ethics in an age of changing technology: familiar territory or new frontiers? *Library Hi Tech,* 17(1)**,** pp.107-113.

CRESWELL, J. W. & PLANO CLARK, V. L. 2007. *Designing and Conducting Mixed Methods Research.* London: Sage.

DE SAULLES, M. & HORNER, D. S. 2011. The portable Panopticon: morality and mobile technologies. *Journal of Information, Communication and Ethics in Society,* 9(3)**,** pp.206-216.

DELEUZE, G. & GUATTARI, F. 1988. *A Thousand Plateaus: Capitalism and Schizophrenia.* London: Continuum.

DEPARTMENT FOR BUSINESS INNOVATION & SKILLS. 2011. *The 2011 Skills for Life Survey: a Survey of Literacy, Numeracy, and ICT Levels in England.* [Online]. Available: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/36000/12-p168-2011-skills-for-life-survey.pdf> [Accessed 01/03/2017].

DI TELLA, R. & SCHARGRODSKY, E. 2004. Do police reduce crime? estimates using the allocation of police forces after a terrorist attack. *American Economic Review,* 94(1)**,** pp.115-133.

DOAN, P. L. 2010. The tyranny of gendered spaces–reflections from beyond the gender dichotomy. *Gender, Place & Culture,* 17(5)**,** pp.635-654.

DOBSON, J. E. & FISHER, P. F. 2007. The Panopticon's changing geography. *Geographical Review,* 97(3)**,** pp.307-323.

DOHERTY, N. F., ANASTASAKIS, L. & FULFORD, H. 2011. Reinforcing the security of corporate information resources: a critical review of the role of the acceptable use policy. *International Journal of Information Management,* 31(3)**,** pp.201-209.

DOWD, R. C. 1990. I want to find out how to freebase cocaine or yet another unobtrusive test of reference performance. *The Reference Librarian,* 11(25/26)**,** pp.483-493.

DOYLE, T. 1998. A Millian critique of library censorship. *The Journal of Academic Librarianship,* 24(3)**,** pp.241-243.

ELLERBROK, A. 2011. Playful biometrics: controversial technology through the lens of play. *The Sociological Quarterly,* 52(4)**,** pp.528-547.

ELO, S. & KYNGÄS, H. 2008. The qualitative content analysis process. *Journal of Advanced Nursing*, 62, pp.107-115.

ELTORAI, A. E. M., NAQVI, S. S., GHANIAN, S., EBERSON, C. P., WEISS, A.-P. C., BORN, C. T. & DANIELS, A. H. 2015. Readability of invasive procedure consent forms. *Clinical and Translational Science,* 8(6)**,** pp.830-833.

ERICSON, R. V. 1997. *Policing the Risk Society.* Oxford: Clarendon Press.

ESLAMIEH, R. 2017. Imposed identity through Foucauldian panopticism and released identity through Deleuzian ressentiment in Samuel Johnson's The History of Rasselas, Prince of Abissinia. *Advances in Language and Literary Studies,* 8(1)**,** pp.125-132.

ESTABROOK, L. S. 1996. Sacred trust or competitive opportunity: using patron records. *Library Journal,* 121(2)**,** pp.48-49.

EUROPOL. 2013. *Cybercrime.* [Online]. Available: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime> [Accessed: 06/10/2015].

EVERETT, C. 2009. Biometrics-based surveillance: Big Brother or vital safeguard? *Computer Fraud & Security,* 2009(11)**,** pp.5-7.

FAIRCLOUGH, N. & WODAK., R. 1997. Critical discourse analysis. In: T.A. DIJK. ed. *Discourse as Social Interaction.* London: Sage.

FAIRCLOUGH, N. 1992. *Discourse and Social Change*. Cambridge: Polity Press.

FAIRCLOUGH, N. 2001a. The discourse of New Labour: Critical discourse analysis. In: S. YATES, S. TAYLOR, & M. WETHERELL. eds. *Discourse as Data: A Guide for Analysis.* London: SAGE.

FAIRCLOUGH, N. 2001b. *Language and Power.* Harlow: Longman Pearson.

FAIRCLOUGH, N. 2010. *Critical Discourse Analysis: The Critical Study of Language.* London: Routledge.

FERNBACK, J. 2013. Sousveillance: communities of resistance to the surveillance environment. *Telematics and Informatics,* 30(1)**,** pp.11-21.

FIGGOU, L. & PAVLOPOULOS, V. 2015. Social psychology: Research methods. In: J.D. WRIGHT. ed. *International Encyclopedia of the Social & Behavioral Science*, (2nd ed). Cambridge: Elsevier.

FITZSIMMONS, P. R., MICHAEL, B. D., HULLEY, J. L. & SCOTT, G. O. 2010. A readability assessment of online Parkinson's disease information. *The Journal of the Royal College of Physicians of Edinburgh,* 40(4)**,** pp.292-6.

FLESCH, R. 1948. A new readability yardstick. *Journal of Applied Psychology,* 32(3)**,** pp.221-233.

FLOWERS, B. F. & RAKES, G. C. 2000. Analyses of acceptable use policies regarding the Internet in Selected K–12 Schools. *Journal of Research on Computing in Education,* 32(3)**,** pp.351-365.

FOLTZ, C. B., PAUL CRONAN, T. & JONES, T. W. 2005. Have you met your organization's computer usage policy? *Industrial Management & Data Systems,* 105(2)**,** pp.137-146.

FOOT, P. 2002. *Virtues and Vices, and Other Essays in Moral Philosophy.* Oxford: Oxford University Press.

FOSKETT, D. J. 1962. *The Creed of a Librarian: No Politics, No Religion, No Morals.* London: Library Association Occasonal Papers No.3.

FOUCAULT, M. 1972. *The Archaeology of Knowledge and The Discourse on Language.* New York: Pantheon.

FOUCAULT, M. 2002. The Eye of Power: A Conversation with Jean-Pierre Barou and Michelle Pierrot. In: T. Levin, U. Frohme, & P. Weibel. eds. *CTRL [+Space]: Rhetorics of Surveillance from Bentham to Big Brother*. Cambrdige, Mass.: MIT Press.

FOUCAULT, M. 1991. *Discipline and Punish: the Birth of the Prison.* London: Penguin.

FRIED, C. 1984. Privacy. In: F.D. SCHOEMAN. ed. *Philosophical Dimensions of Privacy.* Cambridge: Cambridge University Press.

FYFE, N. R. & BANNISTER, J. 1996. City watching: closed circuit television surveillance in public spaces. *Area***,** 28(1) pp.37-46.

GALLAGHER, C., MCMENEMY, D. & POULTER, A. 2015. Management of acceptable use of computing facilities in the public library: avoiding a panoptic gaze? *Journal of Documentation,* 71(3)**,** pp.572-590.

GALLAGHER, M. 2008. Foucault, power and participation. *The International Journal of Children's Rights,* 16(3)**,** pp.395-406.

GALLAGHER, M. 2010. Are schools panoptic? *Surveillance and Society,* 7(3/4)**,** pp.262-272.

GANDY, O. 2007. Data mining and surveillance in the post 9/11 environment. In: S.P. HIER & J. GREENBERG. eds. *The Surveillance Studies Reader.* Maidenhead: Open University Press.

GAUNT, N. 1998. Installing an appropriate Information Security Policy. *International Journal of Medical Informatics,* 49(1)**,** pp.131-134.

GAVISON, R. 1980. Privacy and the limits of law. *The Yale Law Journal,* 89(3)**,** pp.421-471.

GIDDENS, A. 1990. *The Consequences of Modernity.* Cambridge: Polity Press.

GILL, M., & SPRIGGS, A. 2005. *Assessing the Impact of CCTV. Home Office Research Study 292*. London: Home Office Research, Development and Statistics Directorate.

GOMM, R. 2004. *Social Research Methodology: A Critical Introduction*. Basingstoke: Palgrave MacMillan.

GOOLD, B. J. 2002. Privacy rights and public spaces: CCTV and the problem of the "unobservable observer". *Criminal Justice Ethics,* 21(1)**,** pp.21-27.

GORMAN, M. 2015. *Our Enduring Values Revisited : Librarianship in an Ever-Changing World*. Chicago: ALA Editions.

GOTTSCHALK, L. 2007. Internet filters in public libraries: do they belong? *Library Student Journal*. [Online]. Available: <www.librarystudentjournal.org/index.php/lsj/article/view/25/17> [Accessed: 25/11/2017]

GRAHAM, C., REYNARD, J. M. & TURNEY, B. W. 2015. Consent information leaflets – readable or unreadable? *Journal of Clinical Urology,* 8(3)**,** pp.177-182.

GRAVES, W. M. & KEUREN, S. V. 2011. Ancestral Pueblo villages and the panoptic gaze of the commune. *Cambridge Archaeological Journal,* 21(2)**,** pp.263-282.

GRAY, C. J. 2012. Readability: a factor in student research? *The Reference Librarian,* 53(2)**,** pp.194-205.

GRAY, M. 2003. Urban surveillance and panopticism: will we recognise the Facial Recognition Society? *Surveillance and Society,* 1(3)**,** pp.314-330.

GREWAL, P., WILLIAMS, B., ALAGARATNAM, S., NEFFENDORF, J. & SOOBRAH, R. 2012. Quality of vascular surgery Web sites on the Internet. *Journal of Vascular Surgery,* 56(5)**,** pp.1461-1467.

GROOMBRIDGE, N. 2002. Crime control or crime culture TV? *Surveillance & Society,* 1(1)**,** pp.30-46.

GROOMBRIDGE, N. 2008. Stars of CCTV? How the home office wasted millions - A radical 'treasury/audit commission' view. *Surveillance and Society,* 5(1)**,** pp.73-80.

HAGGERTY, K. D. & ERICSON, R. V. 2000. The surveillant assemblage. *The British Journal of Sociology,* 51(4)**,** pp.605-622.

HAMNES, B., VAN EIJK-HUSTINGS, Y. & PRIMDAHL, J. 2016. Readability of patient information and consent documents in rheumatological studies. *BMC Medical Ethics,* 17(1)**,** p.42.

HANSBERRY, D. R., AGARWAL, N., GONZALES, S. F. & BAKER, S. R. 2014. Are we effectively informing patients? A quantitative analysis of on-line patient education

resources from the American Society of Neuroradiology. *American Journal of Neuroradiology,* 35(7)**,** pp.1270-5.

HARNCHARNCHAI, A. & INPLAO, K. 2015. Information ethics and behaviors of upper secondary students regarding the use of computers and the Internet. *Journal of Information Ethics,* 24(1)**,** pp.98-116.

HARPER, L.M. & OLTMANN, S.M., 2017. Big data's impact on privacy for librarians and information professionals. *Bulletin of the Association for Information Science and Technology*, 43(4), pp.19-23.

HARRIS, J. (2011) *School Surveillance: How Big Brother Spies On Pupils. The Guardian*. 9 June. [Online]. Available: < http://www.theguardian.com/uk/2011/jun/09/schools-surveillance-spying-on-pupils> [Accessed: 19/10/2015]

HART, H.L.A., BURNS, J.H. & BENTHAM, J. 1970. *An Introduction to the Principles of Morals and Legislation*. London: Athlone P. Original published 1789.

HASHIMOTO, A. 1979. Measuring the effect of police surveillance on the prevention of traffic accidents. *Accident Analysis & Prevention,* 11(4)**,** pp.261-270.

HAUPTMAN, R. & MOTIN, S. 1994. The Internet, Cyberethics, and Virtual Morality. *The Inverted File,* 18(2)**,** pp.8-9.

HAUPTMAN, R. 1976. Professionalism or culpability? An experiment in ethics. *Wilson Library Bulletin,* 50(8), pp.626-627.

HEDMAN, A. S. 2008. Using the SMOG Formula to revise a health-related document. *American Journal of Health Education,* 39(1)**,** pp.61-64.

HEINS, M., CHO, C. AND FELDMAN, A. 2006. *Internet filters: A public policy report.* [Online]. New York: Brennan Center for Justice. Available: <https://www.brennancenter.org/publication/internet-filters-public-policy-report-2nd-edition> [Accessed 12/07/2017].

HELMRICH, E. V. & HOWERTON, E. D. 2011. Plugging into youth: youth library services in the digital age/era. In: J.C. BERTOT, P.T. JAEGER & C.R. MCCLURE (eds.) *Public*

Libraries and The Internet: Roles, Perspectives, and Implications. Oxford: Libraries Unlimited.

HENDERSON, A. C., HARMAN, S.M., AND HOUSER, J. 2010. A new state of surveillance? An application of Michel Foucault to modern motherhood. *Surveillance and Society,* 7(3/4)**,** pp.231-247.

HENDRICKS, A. 2006. Webmasters, Web Policies, and academic libraries: A Survey. *Library Hi Tech,* 25(1)**,** pp.136-146.

HEOK, A. & LUYT, B., 2010. Imagining the Internet: Learning and access to information in Singapore's public libraries. *Journal of Documentation*, 66(4), pp.475-490.

HERN, A. 2015. I read all the small print on the Internet and it made me want to die. *The Guardian* [Online]. Available: <https://www.theguardian.com/technology/2015/jun/15/i-read-all-the-small-print-on-the-internet> [Accessed 15/06/15].

HEWITT, M. 2000. Confronting the modern city: the Manchester Free Public Library, 1850–80. *Urban History,* 27(1)**,** pp.62-88.

HIER, S. & GREENBERG, J. 2007. *The Surveillance Studies Reader*. Maidenhead: Open University Press.

HIER, S. P. 2003. Probing the Surveillant Assemblage: on the dialectics of surveillance practices as processes of social control. *Surveillance and Society,* 1(3)**,** pp.399-411.

HIMMELFARB, G. 1965. *The Haunted House of Jeremy Bentham*. Durham, N.C.: Duke University Press.

HOEL, T., CHEN, W. & GERGERSEN, A.B. 2018. Are Norwegian academic Librarians ready to share Usage Data for Learning Analytics? *Nordic Journal of Information Literacy in Higher Education*, 10(1), pp.4-17

HOLT, D. B. 2011. LGBTIQ teens—Plugged in and unfiltered: How Internet filtering impairs construction of online communities, identity formation, and access to health information. In: E. GREENBLATT. ed. *Serving LGBTIQ Library and Archives Users:*

Essays on Outreach, Service, Collections and Access. Jefferson, NC: MacFarland & Company Inc.

HOLTHAM, S. 2013. *Is Tate Britain Haunted?* [Online]. Available: <http://www.tate.org.uk/context-comment/blogs/tate-britain-haunted> [Accessed 20/10/2015].

HÖNE, K. & ELOFF, J. H. P. 2002a. Information Security Policy — what do international information security standards say? *Computers & Security,* 21(5)**,** pp.402-409.

HÖNE, K. & ELOFF, J. H. P. 2002b. What makes an effective information security policy? *Network Security,* 2002(6)**,** pp.14-16.

HOUGHTON-JAN, S. 2008. *Internet Filtering Software Tests: Barracuda, CyberPatrol, FilterGate and WebSense*. [Online]. San Jose Public Library.Available: <www.sjlibrary.org/about/sjpl/commission/agen0208_report.pdf> [Accessed: 04/05/2016]

HOWES, L. M., JULIAN, R., KELTY, S. F., KEMP, N. & KIRKBRIDE, K. P. 2014a. The readability of expert reports for non-scientist report-users: Reports of DNA analysis. *Forensic Science International,* 237**,** pp.7-18.

HOWES, L. M., KIRKBRIDE, K. P., KELTY, S. F., JULIAN, R. & KEMP, N. 2013. Forensic scientists' conclusions: How readable are they for non-scientist report-users? *Forensic Science International,* 231(1-3)**,** pp.102-112.

HOWES, L. M., KIRKBRIDE, K. P., KELTY, S. F., JULIAN, R. & KEMP, N. 2014b. The readability of expert reports for non-scientist report-users: Reports of forensic comparison of glass. *Forensic Science International,* 236**,** pp.54-66.

HSIU-FANG HSIEH SARAH E. SHANNON. 2005. Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), pp.1277-1288.

HUANG, P. 2007. How you can protect public access computers. *Computers in libraries,* 27(5)**,** pp.16-20.

ICO. 2017. *The Guide to Freedom of Information*. [Online]. Available: <https://ico.org.uk/for-organisations/guide-to-freedom-of-information/> [Accessed 23/04/2105]

INFOPEOPLE. n.d. *History of Internet Filtering*. [Online]. Available: <https://infopeople.org/content/history-internet-filtering> [Accessed: 06/09/2017]

JAEGER, P. T., MCCLURE, C. R., BERTOT, J. C., & LANGA, L. A. 2005. CIPA: Decisions, implementation, and impacts. *Public Libraries*, 44(2), pp.105-9.

JAEGER, P.T. & BERTOT, J.C. 2011. Shaping the debate: The present and future impacts of policy on the Internet and library servies. In: J.C. BERTOT, P.T. JAEGER & C.R. MCCLURE (eds). *Public libraries and the Internet : Roles, Perspectives, and Implications.* Santa Barbara, Ca.: Libraries Unlimited.

JAMALI, H. R. S., PRIA. 2017. The effects of internet filtering on users' information-seeking behaviour and emotions. *Aslib Journal of Information Management,* 69(4)**,** pp.408-425.

JONES, K. 2017. Learning Analytics, the Academic Library, and Positive Intellectual Freedom. *Journal of Intellectual Freedom and Privacy*, 2(2), pp. 7-10.

JONES, K.M.L.M. & SALO, D., 2018. Learning analytics and the academic library: Professional ethics commitments at a crossroads. *College and Research Libraries*, 79(3), pp.304–323.

JOHANSSON, V. 2004. Public libraries as democratic intermediaries: Some examples from Sweden. *New Library World,* 105(1/2)**,** pp.47-59.

JOHNSON, R. B., ONWUEGBUZIE, A. J. & TURNER, L. A. 2007. Toward a definition of mixed methods research. *Journal of Mixed Methods Research,* 1(2)**,** pp.112-133.

JUZNIC, P., URBANIJA, J., GRABRIJAN, E., MIKLAVC, S., OSLAJ, D. & SVOLJSAK, S. 2001. Excuse me, how do I commit suicide? Access to ethically disputed items of information in public libraries. *Library Management,* 22(1/2)**,** pp.75-80.

KAMEN, M. 2015. *This Graphic Novel makes iTunes T&Cs actually readable*. *Wired* [Online]. Available: <http://www.wired.co.uk/article/itunes-graphic-novel> [Accessed 25/10/16].

KANT, I. 1948. *The Moral Law; Kant's Groundwork of the Metaphysic of Morals*. Trans. H.J. Paton. London: Hutchinson University Library. Original work published 1785.

KASABWALA, K., AGARWAL, N., HANSBERRY, D. R., BAREDES, S. & ELOY, J. A. 2012. Readability assessment of patient education materials from the american academy of otolaryngology—head and neck surgery foundation. *Otolaryngology–Head and Neck Surgery,* 147(3)**,** pp.466-471.

KELEHEAR, Z. 2005. When Email goes bad: be sure that your AUP cover staff as well as students. *American School Board Journal*, (January), pp.32-34.

KELLE, U. 1995. Introduction: an overview of computer-aided methods in qualitative research. In: U. KELLE (ed.) *Computer-aided Qualitative Data Analysis: Theory, Methods, and Practice.* London: Sage.

KLARE, G. R. 2000. The measurement of readability: useful information for communicators. *ACM Journal of Computer Documentation,* 24(3)**,** pp.107-121.

KLINE, M. (1999). Mainstream Loudoun v. Board of trustees of the Loudoun county library. *Berkeley Technology Law Journal*, 14(1), pp.347-370.

KONDILIS, B. K., AKRIVOS, P. D., SARDI, T. A., SOTERIADES, E. S. & FALAGAS, M. E. 2010. Readability levels of health pamphlets distributed in hospitals and health centres in Athens, Greece. *Public Health,* 124(10)**,** pp.547-552.

KOSKELA, H. 2000. 'The gaze without eyes': video-surveillance and the changing nature of urban space. *Progress in Human Geography,* 24(2)**,** pp.243-265.

KOSKELA, H. 2002. 'Cam Era'—the contemporary urban Panopticon. *Surveillance & Society,* 1(3)**,** pp.292-313.

KRANICH, N. (2004). Why filters won't protect children or adults. *Library Leadership & Management*, 18(1), p.14.

KRIPPENDORFF, K. 1989. Content analysis. In E. BARNOUW, G. GERBNER, W. SCHRAMM, T. L. WORTH, & L. GROSS (eds.) *International encyclopedia of* communication, Oxford: Oxford University Press.

KUGAR, M. A., COHEN, A. C., WOODEN, W., THOLPADY, S. S. & CHU, M. W. 2017. The readability of psychosocial wellness patient resources: improving surgical outcomes. *Journal of Surgical Research,* 218**,** pp.43-48.

KUMAGAI, J., & CHERRY, S. (2004). Sensors and sensibility. *IEEE Spectrum*, 41(7), pp.22–26.

LAUGHTON, P. 2008. Hierarchical analysis of acceptable use policies. *South African Journal of Information Management,* 10(4)**,** pp.2-6.

LE GUIN, U. K. 1980. The ones who walk away from Omelas. In: U.K. Le Guin *The Wind's Twelve Quarters. Vol.2.* St Albans: Granada Publishing Limited.

LEE, W. D. & BELDEN, B. R. 1966. A cross-validation readability study of general psychology textbook material and the Dale-Chall readability formula. *The Journal of Educational Research,* 59(8)**,** pp.369-373.

LEONE, M. P. 1995. A historical archaeology of capitalism. *American anthropologist,* 97(2)**,** pp.251-268.

LEVI, M., & WALL, D. S. 2004. Technologies, security, and privacy in the post-9/11 European information society. *Journal of Law and Society*, 31(2), pp.194-220.

LICHTENSTEIN, S. & SWATMAN, P. M. 1997. Internet acceptable usage policy for organizations. *Information Management & Computer Security,* 5(5)**,** pp.182-190.

LIM, A. 2010. The readability of information literacy content on academic library web sites. *Journal of Academic Librarianship,* 36(4)**,** pp.296-303.

LINDUP, K. R. 1995. A new model for Information Security Policies. *Computers & Security,* 14(8)**,** pp.691-695.

LO, K., RAMOS, F. & ROGO, R. 2017. Earnings management and annual report readability. *Journal of Accounting and Economics,* 63(1)**,** pp.1-25.

LONGO, B. 2004. Toward an informed citizenry: readability formulas as cultural artifacts. *Journal of Technical Writing and Communication,* 34(3)**,** pp.165-172.

LUK, A. & ASLANI, P. 2011. Tools used to evaluate written medicine and health information. *Health Education & Behavior,* 38(4)**,** pp.389-403.

LYON, D. 1994. *The Electronic Eye: the Rise of Surveillance Society*. Minneapolis, MN: University of Minnesota Press.

LYON, D. 2001. *Surveillance Society : Monitoring Everyday Life*. Buckingham: Open University Press.

LYON, D. 2002. Everyday surveillance: personal data and social classifications. *Information, Communication & Society,* 5(2)**,** pp.242-257.

LYON, D. 2003. *Surveillance as Social Sorting : Privacy, Risk, and Digital Discrimination.* London: Routledge.

LYON, D. 2006. *Theorizing Surveillance.* London: Routledge.

MANNHEIMER, S., YOUNG, S.W.H & ROSSMANN, D. 2016. On the ethics of social network research in libraries. *Journal of Information, Communication and Ethics in Society*, 14(2), pp.139-151.

MARCO, G. (1996). Ethics for librarians: a narrow view. *Journal of Librarianship and Information Science*, 28(1), pp.33-38.

MARKUS, T., A. 1993. *Buildings & Power: Freedom and Control in the Origin of Modern Building Types.* London: Routledge.

MARX, G. 2006. Soft surveillance: The growth of mandatory volunteerism in collecting personal information – 'Hey buddy can you spare a DNA?'. In: T. MONAHAN. ed. *Surveillance and Security: Technological Politics and Power in Everyday Life.* London: Routledge.

MARX, G. 2007. What's new about the 'New Surveillance'? Classifying for change and continuity. In: S.P. HIER & J. GREENBERG. eds. *The Surveillance Studies Reader.* Maidenhead: Open University Press.

MASROM, M., MAHMOOD, N. H. N., & ZAINON, O. 2013. Cyberethics and Internet behaviour of Malaysian primary education students. *Journal of Emerging Trends in Educational Research and Policy Studies*, 4(1), pp.104-111.

MATHIESEN, T. 1997. The viewer society: Michel Foucault's `Panopticon' revisited. *Theoretical Criminology,* 1(2)**,** pp.215-234.

MAY, J. 2014. What's the best way to keep children safe online? *CILIP Blog*. 27 January. Online. Available: < https://archive.cilip.org.uk/blog/what-s-best-way-keep-children-safe-online> [Accessed 24/03/2019]

MAYRING, P. 2000. Qualitative Content Analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 1(2), [ONLINE] Available: <http://nbn-resolving.de/urn:nbn:de:0114-fqs0002204> [Accessed: 20/05/19]

MCCAHILL, M. & NORRIS, C. 2002. *On the Threshold to Urban Panopticon? Analysing the Empoyment of CCTV in European Cities and Assessing its Social and Political Impact.* Berlin: Urban Eye.

MCLAUGHLIN, G. H. 1969. SMOG grading-a new readability formula. *Journal of reading,* 12(8)**,** pp.639-646.

MCMENEMY, D. & BURTON, P. F. 2005. Managing access: legal policy and issues of ICT use. In: D. MCMENEMY, & A. POULTER. eds. *Delivering Digital Services: a Handbook for Public Libraries and Learning Centres.* London: Facet.

MCMENEMY, D. 2008. Internet access in UK public libraries: notes and queries from a small scale study. *Library Review,* 57(7)**,** pp.485-489.

MCMENEMY, D. 2009. *The Public Library.* London: Facet.

MCMENEMY, D. 2014. Towards a public library standard for acceptable use of computing facilities. *IFLA WLIC 2014 - Lyon - Libraries, Citizens, Societies: Confluence for Knowledge in Session 72 - Committee on Standards.* In: IFLA WLIC 2014, Lyon, France: IFLA.

MCMENEMY, D. 2016. *Digital Ethics : A UKeiG White Paper*. [Online]. Available: <https://archive.cilip.org.uk/system/files/documents/digital_ethics_white_paper_final.pdf> [Accessed 15/04/2017] UKeiG.

MCNEILL, P. & CHAPMAN, S. 2005. *Research Methods.* London: Routledge.

MEIKLEJOHN, A. 1961. The First Amendment is an absolute. *The Supreme Court Review,* 1961**,** pp.245-266.

MILL, J. S. 1985. *On Liberty.* Harmondsworth: Penguin. Original published 1859.

MILLER, J.A. & MILLER. R. 1987. Jeremy Bentham's panoptic device. *October*, 41(Summer, 1987), pp.3–29.

MILTON, J. 1973. *Areopagitica : a Speech ... for the Liberty of Unlicensed Printing to the Parliament of England.* Reprint. Cambridge: Deighton Bell. Original work published 1644.

MINOW, M. 1997. Filters and the public library: A legal and policy analysis. *First Monday*, 2(12). p.1.

MONAHAN, T. 2011. Surveillance as cultural practice. *The Sociological Quarterly,* 52(4)**,** pp.495-508.

MOORE, A. D. 2003. Privacy: its meaning and value. *American Philosophical Quarterly,* 40(3)**,** pp.215-227.

MOORE, B. 1998. Privacy. *Society,* 35(2)**,** pp.287-299.

MOOREFIELD-LANG, H.M. (2015) User agreements and makerspaces: a content analysis. *New Library World*, 116(7/8), pp.358-368

MORRIS, B. W., KLEIST, V. F., & DULL, R. B. 2013. Considering information system acceptable use policies and ethical issues. *IMA Education Case Journal*, 6(3), Article 2.

MORRIS, N. & ROTHMAN, D. J. 1995. *The Oxford History of the Prison: The Practice of Punishment in Western Society*. Oxford: Oxford University Press.

MUNDAY, R. 1994. Bentham's Prison: A Study of the Panopticon Penitentiary by Janet Semple (Review). *The Cambridge Law Journal,* 53(1)**,** pp.167-169.

MUSWAZI, P. 2009. Usability of university library home pages in Southern Africa: a case study. *Information Development,* 25(1)**,** pp.51-60.

NAGEL, T. 1995. Personal rights and public space. *Philosophy & Public Affairs,* 24(2)**,** pp.83-107.

NATIONAL LITERACY TRUST. 2017a. *Adult Literacy: How Many Illiterate Adults are There in England?* [Online]. Available: <http://www.literacytrust.org.uk/adult_literacy/illiterate_adults_in_england> [Accessed 08/02/2017].

NATIONAL LITERACY TRUST. 2017b. *How Can I Assess the Readability of My Document Or Write More Clearly?* [Online]. Available: <http://www.literacytrust.org.uk/about/faqs#q710> [Accessed 08/02/2017].

NATIONAL RESEARCH COUNCIL. 2002. *Youth, Pornography, and the Internet.* Washington, DC: National Academies Press.

NEWELL, B. C., & RANDALL, D. P. (2013). Video Surveillance in Public Libraries: A Case of Unintended Consequences? In *System Sciences (HICSS), 2013 46th Hawaii International Conference on System Sciences* pp. 1932–1941. IEEE.

NISSENBAUM, H. F. 2010. *Privacy In Context : Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford Law Books.

NORRIS, C. & ARMSTRONG, G. 1999. *The Maximum Surveillance Society: the Rise of CCTV*. Oxford: Berg.

NORRIS, C. & MCCAHILL, M. 2006. CCTV: beyond penal modernism? *The British Journal of Criminology,* 46(1)**,** pp.97-118.

NORRIS, C., MCCAHILL, M. & WOOD, D. 2004. Editorial. The growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance and Society,* 2(2/3)**,** pp.110-135.

OLSSON, M. R. 2010. Michel Foucault: discourse, power/knowledge and the battle for truth. In: G.J. LECKIE, L.M. GIVEN & J.E. BUSCHMAN. eds. *Critical Theory for Library and Information Science.* California: Libraries Unlimited.

ORLIKOWSKI, W. J. & BAROUDI, J. J. 1991. Studying Information Technology in organizations: research approaches and assumptions. *Information Systems Research,* 2(1)**,** pp.1-28.

PALGI, R. D. 1996. Rules of the road: why you need an acceptable use policy. *School Library Journal,* 42(8)**,** pp.32-33.

PATON, G. (2014) *Classrooms Put Under 'Permanent Surveillance' By CCTV. The Telegraph*. 20 April. [Online]. Available at <

http://www.telegraph.co.uk/education/educationnews/10776060/Classrooms-put-under-permanent-surveillance-by-CCTV.html> [Accessed: 20/10/2015]

PAUTZ, H. 2013. Managing access to the internet in public libraries. *New Library World,* 114(7/8)**,** pp.308-318.

PAYNE, D. (2016) *New research maps the extent of web filtering in public libraries*. [Online]. Available <http://www.cilip.org.uk/blog/new-research-maps-extent-web-filtering-public-libraries> [Accessed 23/03/2019].

PENNEY, J. W. 2016. Chilling effects: online surveillance and Wikipedia use. *Berkeley Technology Law Journal*, 31(1), pp.117-182.

PICKFORD, J. A. 2013. *Research Methods in Information.* London: Facet.

PIDAPARTHY, U. 2011. *What You Should Know About iTunes' 56-Page Legal Terms.* [Online]. CNN. Available: <http://edition.cnn.com/2011/TECH/web/05/06/itunes.terms/> [Accessed 25/10/16].

PORS, N. O. 2001. Misbehaviour in the public library: Internet use, filters and difficult people. *New Library World,* 102(9), pp.309-313.

POST, R. 1993. Managing deliberation: the quandary of democratic dialogue. *Ethics,* 103(4)**,** pp.654-678.

POULTER, A. 2005. *The Library and Information Professional's Internet Companion : a practical Resource for Library and Information Professionals*. London: Facet.

POULTER, A., FERGUSON, I. , MCMENEMY, D. AND GLASSEY, R.J. 2009. Question: where would you go to escape detection if you wanted to do something illegal on the internet? Hint: shush! In: H.H. JAHANKHANI & F. HSU. eds. *Global Security, Safety and Sustainability: 5th International Conference, ICGS3. Communications in Computer and Information Science (1st).* London: Springer-Verlag.

PRIKS, M. 2014. Do surveillance cameras affect unruly behavior? A close look at grandstands. *The Scandinavian Journal of Economics,* 116(4)**,** pp.1160-1179.

PRIOR, L. 2011. *Using Documents and Records in Social Research.* London: Sage.

PRZYBYLSKI, A.K. & NASH, V. 2017. Internet filtering technology and aversive online experiences in adolescents. *The Journal of Pediatrics*, 184, pp.215-219.

PRZYBYLSKI, A.K. & NASH, V. 2018. Internet filtering and adolescent exposure to online sexual material. *Cyberpsychology, Behavior, and Social Networking*, 21(7), pp.405-410.

QSR INTERNATIONAL. 2015. *About Nodes.* [Online] Available: <http://help-nv11.qsrinternational.com/desktop/concepts/about_nodes.htm> [Accessed: 20/03/2016]

RAJPOOT, Q.M. & JENSEN, C.D. 2015. Video surveillance: Privacy issues and legal compliance. In: V. KUMAR, & J. SVENSSON. eds. *Promoting Social Change and Democracy through Information* Technology. IGI global.

RANDALL, D. & NEWELL, B. 2014. The panoptic librarian: The role of video surveillance in the modern public library*. Proceedings of the 2014 iConference*. pp.508-21.

RANGANATHAN, S. R. 1957. *The Five Laws of Library* Science. London: Madras.

REEVES, A. 1998. The panopticisation of shopping: CCTV and leisure consumption In: C. NORRIS, J. MORAN & G. ARMSTRONG. eds. *Surveillance, Closed Circuit Television and Social Control*. Aldershot: Ashgate.

REIMAN, J. H. 1995. Driving to the Panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara Computer and High Technology Law Journal,* 11(1)**,** pp.27-44.

RESNICK, P., HANSEN, D. & RICHARDSON, C. 2004. Calculating error rates for filtering software. *Communications of the ACM,* 47(9)**,** pp.67-71.

ROSE, N. S. 1999. *Powers of Freedom : Reframing Political Thought.* Cambridge: Cambridge University Press.

RUDALL, P. 1984. Taxonomic and evolutionary implications of rhizome structure and secondary thickening in Iridaceae. *Botanical Gazette,* 145(4)**,** pp.524-534.

RUDD, R. E. 2010. *Harvard School of Public Health: Health Literacy* [Online]. Available: <https://www.hsph.harvard.edu/healthliteracy/assessing-materials/> [Accessed: 7/7/17].

RUIGHAVER, A. B., MAYNARD, S. B. & WARREN, M. 2010. Ethical decision making: improving the quality of acceptable use policies. *Computers & Security,* 29(7)**,** pp.731-736.

RUSK, M. 2001. Acceptable use policies: four examples from community college libraries. *Community & Junior College Libraries,* 10(2)**,** pp.83-90.

SAFA, N. S., VON SOLMS, R., & FURNELL, S. 2016. Information security policy compliance model in organizations. *Computers & Security*, 56, pp.70-82.

SANDEL, M. J. 2010. *Justice : What's the Right Thing to Do?* London: Penguin.

SANNA, T., KIMMO, T. & REIJO, S. 2005. “Isms” in information science: constructivism, collectivism and constructionism. *Journal of Documentation,* 61(1)**,** pp.79-101.

SAUL, H. (2015). *GoPro Camera Films Man as He is Robbed at Gun Point in Cape Town. The Independent.* 17 February. [Online]. Available: < http://www.independent.co.uk/news/world/gopro-camera-films-man-as-he-is-robbed-at-gun-point-in-cape-town-9495059.html> [Accessed: 19/10/2015]

SAVAGE, A. & HYDE, R. 2014. Using freedom of information requests to facilitate research. *International Journal of Social Research Methodology,* 17(3)**,** pp.303-317.

SCALES, P. 2009. Better safe than sorry: does your library have an online acceptable-use policy? *School Library Journal,* 55(3)**,** p.22.

SCHAUER, F. 1978. Fear, risk and the first amendment: unraveling the chilling effect. *Boston University Law* Review, 58(5), pp.685-732.

SCHAUER, F. F. 1982. *Free Speech : a Philosophical Enquiry.* Cambridge: Cambridge University Press.

SCHOFIELD, P. 2009. *Bentham: a Guide for the Perplexed.* London: Continuum.

SCHOLTZ, P. 2001. *Internal Security: Rules and Risks. New Architect: Web Techniques.* Online. Available: <https://people.apache.org/~jim/NewArchitect/webtech/2001/07/sholtz/index.html> [Accessed: 24/10/2016]

SCOTT, T. J. & VOSS, R. B. 1994. Ethics and the 7 “P's” of computer use policies. *ECA 1994 Proceedings of the Conference on Ethics in the Computer Age*. pp.61-67.

SEELY, J. 2013. *The Oxford Guide to Effective Writing and Speaking*. Oxford: Oxford University Press.

SEMPLE, J. 1993. *Bentham's Prison a Study of the Panopticon Penitentiary.* Oxford: Clarendon.

SHIRAZI, F. & GREENAWAY, K. 2009. Examining validity claims for internet filtering in Islamic Middle Eastern countries: a critical discourse analysis. *AMCIS 2009 Proceedings***,** 794.

SHIRAZI, F. 2012. Free and open source software versus Internet content filtering and censorship: a case study. *Journal of Systems and Software,* 85(4)**,** pp.920-931.

SHIRAZI, F., NGWENYAMA, O. & MORAWCZYNSKI, O. 2010. ICT expansion and the digital divide in democratic freedoms: an analysis of the impact of ICT expansion, education and ICT filtering on democracy. *Telematics and Informatics,* 27(1)**,** pp.21-31.

SIAU, K., NAH, F. F.-H. & TENG, L. 2002. Acceptable internet use policy. *Communications of the ACM, 45***,** pp.75-79.

SIEMENS, G. 2012. Learning analytics: Envisioning a research discipline and a domain of practice. Paper presented at the Second International Conference on Learning Analytics and Knowledge, Vancouver.

SIGLER, K., JAEGER, P. T., BERTOT, J. C., MCDERMOTT, A. J., DECOSTER, E. J. & LANGA, L. A. 2011. The role of public libraries, the Internet, and economic uncertainty. *Advances in Librarianship,* 34**,** pp.19-35.

SKAGGS, J. A. 2002. Burning the library to roast the pig? Online pornography and Internet Filtering in the free public library. *Brooklyn Law Review,* 68(3)**,** pp.809-852.

SMITH, B. A. & HESSE-BIBER, S. 1996. Users' Experiences with qualitative data analysis software: neither Frankenstein's Monster nor muse. *Social Science Computer Review,* 14(4)**,** pp.423-432.

SMITH, D. & PROTEVI, J. 2018. *Gilles Deleuze* [Online]. Available: <https://plato.stanford.edu/archives/spr2018/entries/deleuze/> [Accessed 16/05/2016].

SMITH, E. A. & KINCAID, J. P. 1970. Derivation and validation of the Automated Readability Index for use with technical materials. *Human Factors,* 12(5)**,** pp.457-564.

SOBEL, D.L. 2003. Internet filters and public libraries. In *First Reports Vol. 4 No. 2.* South Nashville, Tennessee: Vanderbilt University, First Amendment Center. [Online]. Available:< http://www.Firstamendmentcenter.org/Madison/Wp-Content/Uploads/2011/03/Internetfilters.pdf> [Accessed: 20/10/2015]

SOLOVE, D. J. (2002) Digital dossiers and the dissipation of fourth amendment privacy, *Southern California Law Review*, 75(1), pp.1083−1169.

SOVERN, J. 1999. Opting in, opting out, or no options at all: the fight for control of personal information. *Washington Law Review*, 74(4), pp.1033-1118.

SPACEY, R., COOKE, L., CREASER, C. & MUIR, A. 2014. *Managing Access to the Internet in Public Libraries [MAIPLE]*. Loughborough, Leicestershire: LISU. [Online]. Available: https://www.lboro.ac.uk/microsites/infosci/lisu/maiple/downloads/maiple-report.pdf [Accessed: 25/03/2019]

SPACEY, R., COOKE, L., CREASER, C. & MUIR, A. 2015. Regulating Internet access and content in UK public libraries: findings from the MAIPLE project. *Journal of Librarianship and Information Science,* 47(1)**,** pp.71-84.

SPEARS, R. & LEA, M. 1994. Panacea or Panopticon?: the hidden power in computer-mediated communication. *Communication Research,* 21(4)**,** pp.427-459.

SPINELLO, R. A. 2016. *Cyberethics: Morality and Law in Cyberspace*. Burlington, MA: Jones & Bartlett Learning.

SPURLIN, C.J., & GARRY, P.M. 2009. Does filtering stop the flow of valuable information? A case study of the Children's Internet Protection Act (CIPA) in South Dakota. *South Dakota Law Review*, 54(1), pp.89-96.

STAHL, B. C. 2007. Privacy and security as ideology. *IEEE Technology and Society Magazine,* 26(1)**,** pp.35-45.

STEWART, F. 2000. Internet acceptable use policies: navigating the management, legal, and technical issues. *Information Systems Security,* 9(3)**,** pp.1-7.

STORY, L. & STONE, B. 2007. *Facebook Retreats on Online Tracking. The New York Times*. November 30. [Online]. Available: <http://www.nytimes.com/2007/11/30/technology/30face.html?_r=0> [Accessed: 20/10/2015]

STOYCHEFF, E. 2016. Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring. *Journalism & Mass Communication Quarterly*, 93(2), pp.296–311.

STURGES, P., DAVIES, E., DEARNLEY, J., ILIFFE, U., ILIFFE, U., OPPENHEIM, C. & HARDY, R. 2003. User privacy in the digital library environment: an investigation of policies and preparedness. *Library Management,* 24(1)**,** pp.44-50.

STURGES, R. P. 2002. *Public Internet Access in Libraries and Information Services.* London: Facet.

SVIDER, P. F., AGARWAL, N., CHOUDHRY, O. J., HAJART, A. F., BAREDES, S., LIU, J. K. & ELOY, J. A. 2013. Readability assessment of online patient education materials from academic otolaryngology–head and neck surgery departments. *American Journal of Otolaryngology--Head and Neck Medicine and Surgery,* 34(1)**,** pp.31-35.

TARIQ, S. & WOODMAN, J. 2013. Using mixed methods in health research. *Journal of the Royal Society of Medicine Short Reports,* 4(6), pp.1-8.

TAVANI, H. T. 2007. Regulating cyberspace: concepts and controversies. *Library Hi Tech,* 25(1)**,** pp.37-46.

TAYLOR, E. 2010. Evaluating CCTV: why the findings are inconsistent, inconclusive and ultimately irrelevant. *Crime Prevention and Community Safety,* 12(4)**,** pp.209-232.

TESCH, R. 1990. *Qualitative Research: Analysis Types and Software Tools*. Bristol, PA: Falmer Press.

TRUSHINA, I. 2004. Freedom of access: ethical dilemmas for internet librarians. *The Electronic Library,* 22(5)**,** pp.416-421.

UCL. 2010. *The Panopticon* [Online]. Available: <https://www.ucl.ac.uk/bentham-project/who/panopticon> [Accessed 20/10/2015].

UNAR, J. A., SENG, W. C. & ABBASI, A. 2014. A review of biometric technology along with trends and prospects. *Pattern Recognition,* 47(8)**,** pp.2673-2688.

VAISMORADI, M, TURUNEN, H. & BONDAS, T. 2013. Qualitative descriptive study. *Nurs Health Sci*, 15, pp.398-405.

VAN DEN HOVEN, J., BLAAUW, M., PIETERS, W. & WARNIER, M. 2016. *Privacy and Information Technology*. The Stanford Encyclopedia of Philosophy. [Online]. Available: <https://plato.stanford.edu/archives/spr2016/entries/it-privacy/> [Accessed 06/05/2016].

VARGAS, C.R., CHUANG, D.J., GANOR, O., & LEE, B.T. 2014. Readability of online patient resources for the operative treatment of breast cancer. *Surgery*, 156(2), pp.311-318.

VON HIRSCH, A. 2000. The ethics of public television surveillance. In: A. VON HIRSCH, D. GARLAND & A. WAKEFIELD. eds. *Ethical & Social Perspectives on Situational Crime Prevention.* Oxford: Hart.

WAHL-JORGENSEN, K., BENNETT, L. & TAYLOR, G. 2017. The normalization of surveillance and the invisibility of digital citizenship: Media debates after the Snowden revelations. *International Journal of Communication*. 11, pp.740-762.

WAINWRIGHT, M. 2003. *New Weapon in Fight Against Street Crime*. *The Guardian*. 6 November. Online. Available: <

http://www.Theguardian.Com/Uk/2003/Nov/06/Ukcrime.Martinwainwright> [Accessed: 20/10/2015]

WALTERS, K. A. & HAMRELL, M. R. 2008. Consent forms, lower reading levels, and using Flesch-Kincaid readability software. *Therapeutic Innovation & Regulatory Science,* 42(4)**,** pp.385-394.

WANG, L.-W., MILLER, M. J., SCHMITT, M. R. & WEN, F. K. 2013. Assessing readability formula differences with written health information materials: Application, results, and recommendations. *Research in Social and Administrative Pharmacy,* 9(5)**,** pp.503-516.

WARREN, S. D. & BRANDEIS, L. D. 1890. The Right to Privacy. *Harvard Law Review,* 4(5)**,** pp.193-220.

WEBER, R. 1990. *Quantitative Applications in the Social Sciences: Basic Content Analysis*. Thousand Oaks, CA: SAGE Publications, Inc.

WERRETT, S. 1999. Potemkin and the Panopticon: Samuel Bentham and the architecture of absolutism in eighteenth century Russia. *Journal of Bentham Studies,* 2**,** pp.1-25.

WESTIN, A. 1967. *Privacy and Freedom*. New York: Atheneum.

WILLARD, N., 2012. *Cyber savvy: Embracing digital safety and civility*. Thousand Oaks: Corwin Press.

WILLIAMSON, K., GIVEN, L.M. & SCIFLEET, P. 2018. Qualitative data analysis. In: K. WILLIAMSON, G.JOHANSON. eds. *Research Methods*. (2nd ed) Cambridge: Chandos.

WILLSON, J. & OULTON, T. 2000. Controlling access to the Internet in UK public libraries. *OCLC Systems & Services: International Digital Library Perspectives,* 16(4)**,** pp.194-201.

WILSON, W. M., ROSENBERG, L. H. & HYATT, L. E. 1997. Automated analysis of requirement specifications. *Proceedings of the 19th International Conference on Software Engineering.* Boston, Massachusetts, USA: ACM.

WONG, K. & LEVI, J. R. 2016. Partial tonsillectomy: Content and readability of online health information. *The Annals of Otology, Rhinology, and Laryngology,* 126(3)**,** pp.192-8.

WOOD, D. 2003. Editorial. Foucault and panopticism revisited. *Surveillance and Society,* 1(3)**,** pp.234-239.

.WOODWARD, J. A. 2007. *What Every Librarian Should Know About Electronic Privacy*. London: Libraries Unlimited.

WYATT, A. M. 2006. Do librarians have an ethical duty to monitor patrons' internet usage in the public library? *Journal of Information Ethics,* 15(1)**,** pp.70-79.

YOUNG, S. 1997. Perspectives on... Sexually-explicit materials via the internet: ethical concerns for the library profession. *The Journal of Academic Librarianship,* 23(1)**,** pp.49-50.

ZHANG, Y. & WILDEMUTH, B. M. 2016. Qualitative analysis of content. In: B.A. WILDMUTH. ed. *Applications of Social Research Methods to Questions in Information and Library Science* (2nd ed.) Oxford: Pearson Education.

ZIMMER, M. 2010. 'But the data is already public': on the ethics of research in Facebook. *Ethics and Information Technology*, 12(4), pp. 313–325.

ZIMMER, M. 2013. Patron privacy in the "2.0" era: Avoiding the Faustian bargain of library 2.0. *Journal of Information Ethics*, 22(1), pp.44-59.

ZURAWSKI, N. 2011. Local practice and global data: loyalty cards, social practices, and consumer surveillance. *The Sociological Quarterly,* 52(4)**,** pp.509-527.

9.1 Court cases

Kathleen R. v City of Livermore [2001] 87 Cal. App. 4th 684

Katz v. United States [1967] 389 U.S. 347

Olmstead v. United States [1928] 277 U.S. 438

United States v. American Library Association [2003] 539 U.S. 194

Whitney v. California [1927] 274 U.S. 357

Appendix 1. Coding Framework

Theme: Panopticism and Lyon		
Sub-Category	**Definition and Coding Rules**	**Example**
Monitoring Care	Surveillance as protection or care Monitoring is framed as benevolent, often with words such as “safe”	In order to ensure a safe enjoyable experience for all of our members, we operate a robust monitoring and filtering practice at all times. This practice operates both electronically and manually
Monitoring Control	Surveillance as disciplinary/controlling Surveillance is used to ensure rules are followed	Use of the Internet will be monitored to ensure that it is not being used improperly.
Monitoring Neutral	Neither caring nor controlling Surveillance is used but is neutral	We use software to monitor and filter all use of the internet on public computers
Not Monitoring	Monitoring is explicitly not used	[NAME REMOVED] does not monitor your email or other communications electronically
Panoptic Gaze	Surveillance is unverifiable Surveillance is descried as random	Users should be aware that all public internet access is monitored, and that random checks will be made on sites visited
General Care	Protective or caring Statements of protection; safeguarding	The following policy has been developed in order to safeguard both users and their interests
General Control	Statements of control	Access is controlled
Compliance	Following rules Using words such as abide; comply; obey; must	Every time you log into the Council’s network you are agreeing to abide by its policies

Discipline	Sanctions: banning; suspension; punishment	Any individual found engaged in any inappropriate activity as defined above will have their access withdrawn
Power and authority	Discussion of power relationships Promotion of the idea of power	The Council's decision as to which websites fall into these categories is final
Theme: Sturges elements of an AUP		
Sub-Category	**Definition and Coding Rules**	**Example**
Aims and Objectives	Why the service is there, what it seeks to accomplish	[NAME REMOVED] Libraries provides computer and internet access and Wifi as part of its role of enabling access to cultural and educational information and resources
Eligibility Full	Who can use the service Description of who can use the service Coded as full if it gives details in depth	All users of this service are strongly encouraged to register as a member of the library as this will allow access to the automatic PC booking system… If you do not wish to be a member of [NAME REMOVED] Libraries and you wish to book a PC you will have to pay to a small charge… Children under the age of 12 are encouraged to be library members but are not subject to any charges
Eligibility partial	Who can use the service Description of who can use the service Coded as partial if it only gives some information	Users under 16 can only use these computers if a Parental Consent Form has been signed by their parent or carer

Scope	Facilities provided by the library This includes if the facility is for study use only and if there are limits on the service	The services are not designed to support business or commercial activities
Unacceptable use	What is not allowed by the service	Users must behave in a manner that is conducive to learning; excessive volume levels and disruptive behaviour will not be tolerated. Any individual or group who displays such behaviour will be asked to leave
Illegal Use	Illegal usage of facilities	The Telecommunications Act 1984 makes it an offence to transmit, over telephone lines in England and Wales, a message or any other material that is grossly offensive or of indecent, obscene or menacing character
Service Commitments	What levels of service are provided This includes disclaimers regarding the accuracy of the Internet	The Internet offers unlimited global access to information and [NAME REMOVED] Library & Information Services will not be held responsible for the accuracy, validity, legality or usefulness of information accessed on-line. Nor can it be held accountable for any unacceptable or inappropriate use made by an individual
User commitments	What the library requires of the user	DECLARATION: I agree that I will not access or distribute material which is unlawful, indecent or violent and which may be deemed to be offensive to other library users and contravene English Law, or to use any software not provided by the Authority. I understand that

		if I do not comply with these terms and conditions, or if I misuse Council equipment in any way, I will no longer have access to computers in any [NAME REMOVED] library
Theme: Filtering		
Sub-Category	**Definition and Coding Rules**	**Example**
Filtering In use	Filtering is explicitly stated as being in use	[NAME REMOVED] operates filtering software to guard against illegal and offensive sites
Filtering levelled	Filtering is explicitly stated as being in use and has different levels depending on age	The Internet facilities are filtered, with a high level of filtering for children's access and a lower level of filtering for adult users
Filtering Children only	Filtering is explicitly stated as being in use and is only used for children's access	Content is filtered for children's access. There is no Internet filtering for adults
Not in use	Filtering is explicitly mentioned as not being in use	There is no Internet filtering for users
Unclear	Filtering has been used, but is not explicitly mentioned or in non-transparent – pages are described as blocked but with no prior information on filtering has been made	If you cannot access a website as it is blocked, please speak to a member of staff to request it be released for access (subject to checks)
Unblocking information	Guidelines on what to do if a patron comes across a blocked page	If a customer feels that the filtering system is blocking a site unnecessarily or that access to a site should be blocked they should contact a member of staff and ask to complete a review form so that further investigation can be carried out by the library management
Efficacy	Details of how reliable filtering software or acknowledging it may not	The internet service is filtered in order to block access to websites known

	block all websites or erroneously block websites	to contain illegal, offensive and/or unsuitable content. Some legitimate sites may be blocked as a result of the filtering activity and other inappropriate sites may inadvertently be made available prior to their being blocked
Theme: CILIP's ethical principles		
Sub-Category	**Definition and Coding Rules**	**Example**
CILIP Principle 1 Concern for the public good in all professional matters, including respect for diversity within society, and the promoting of equal opportunities and human rights	Supporting the needs of the community; promoting human rights	If you have special needs for accessing the computers, please let us know and we will do our best to help you
CILIP Principle 2 Concern for the good reputation of the information profession	Statements pertaining to the upholding of reputation of the information profession	The Libraries and Arts Service recognises that it is only through continued public confidence in the upholding of data protection principles that confidence in the library itself can be maintained, which is vital to the library's role in the community and the community's right to know
CILIP Principle 3 Commitment to the defence, and the advancement, of access to information, ideas and works of the imagination	Statements supporting access to information	[NAME REMOVED] Council provides public access to Internet services for its citizens and customers as part of its objective to ensure the maximum amount of access to knowledge, information and collaboration by its citizens and customers
CILIP Principle 4 Provision of the best possible service within available resources	Statements of commitment to access provision and making sure resources were spread amongst users to	Please ensure that you have completed your session within your allotted time in order that all users

	allow for fullest possible access	can enjoy this facility to the full
CILIP Principle 5 Concern for balancing the needs of actual and potential users and the reasonable demands of employers	Statements referring to needs of users, as well as local authority	When making decisions on blocking access to websites, [NAME REMOVED] Libraries recognises the need to reconcile the conflicting values of maintaining and defending freedom of access to information, protecting others from harm, and obtaining best value from the Council's investment
CILIP Principle 6 Equitable treatment of all information users	Statements referring to equal treatment of all users	All members of the public are entitled to use the computer facilities provided by [NAME REMOVED] Council at the designated sites. The Council believes that the public are entitled to access the Internet for their informational, educational and leisure needs on payment of the appropriate fee (where applicable)."
CILIP Principle 7 Impartiality, and avoidance of inappropriate bias, in acquiring and evaluating information and in mediating it to other information users	Statements referring to dissemination of information, allowing for patrons to access a wide range of materials	[NAME REMOVED] provides public access to Internet services for its citizens and customers as part of its objective to ensure the maximum amount of access to knowledge, information and collaboration by its citizens and customers
CILIP Principle 8 Respect for confidentiality and privacy in dealing with information users	Statements referring to respecting and dealing with patron privacy	[NAME REMOVED] recognizes the position of special trust that libraries have with members of the public. This statement clarifies policy and practice with regard to confidential information about users (and their use of library resources) that comes into

		[NAME REMOVED]s' possession.
CILIP Principle 9 Concern for the conservation and preservation of our information heritage in all formats	Maintaining and protecting information formats	3. Users may use only software provided for the purpose by [NAME REMOVED] Libraries and must not alter, amend or delete any of the programmes or settings already resident on the computer's internal fixed disk or in its memory.
CILIP Principle 10 Respect for, and understanding of, the integrity of information items and for the intellectual effort of those who created them	Statements referring to the protection of information items, including intellectual property	• Copyright The scanning of copyright material is only legal for the purpose of private study and/ or research and for other non-commercial purposes. In all other cases prior permission from the copyright owners must be obtained by the user. Wherever possible the source of the material should be acknowledged
CILIP Principle 11 Commitment to maintaining and improving personal professional knowledge, skills and competences	Statements referring to staff such as training etc.	Our aim is to widen participation, support lifelong learning, provide information in a wide range of formats and give equal access to all users. We are also committed to an ongoing staff training programme which will respond to the needs of internet users.
CILIP Principle 12 Respect for the skills and competences of all others, whether information professionals or information users, employers or colleagues	Statements reflecting respect for the skills of others	No examples (category not found in AUPs)

Appendix 2. Model Policy

Welcome

Welcome to [NAME] Library Service. The library is a vital part of the local community. It provides information access and a connection to the Internet. We aim to provide a safe and pleasant space for everyone. These services are for personal use – for study and for recreation. This policy has been created as a guide for users.

We encourage users to use all aspects of our ICT facilities. At [NAME] we provide the following services:

- ***Internet access***
- ***Email access***
- ***Printing***

Please ask staff for details regarding access requirements.

Who can use this service?

This service is available for all residents of [AREA NAME]. Those who are visiting [AREA NAME] can use a guest login. Ask for a form from one of our staff members. Please have your ID handy.

We encourage children to use these facilities. For those over 16 access is available on all computers. For those 16 and under we require a form signed by a guardian. We ask that adults supervise those under 12.

We provide this service free of charge in one-hour sessions. You can use any available PC. You can also book your session in advance. Feel free to extend your time if no-one is waiting by asking our staff.

Usage and filtering

We provide these facilities for recreation and study. Email and chat room access is available. You can download resources, and shop online. Please take care when you

are using the Internet. Only give out personal information to those you trust. If you feel unsure please ask a member of staff. Printing is available, at the cost of 10p per page. Please keep noise to a minimum so all users may have a pleasant experience.

To ensure Internet access is safe for all, we use a filtering service. Filtering software blocks websites that may be harmful or offensive. A notice will appear on screen if you access a filtered website. Users who are 12 and under have a higher level of filtering. In the case of those over 18, a non-filtered service is available as well.

A filtering list can be found at the end of this Policy.

Please note that filtering is not fool proof. Filtering can block websites or let through websites by mistake. Adults should make sure to supervise their child's use of the Internet. If you find a filtering error, please tell our staff. You can also email, webform, or post a note in the comments box. We treat all suggestions with the strictest confidence.

Misuse

We aim to provide a safe environment for everyone. As such, certain uses which may harm others is not allowed. This includes illegal use of the service such as:

- ***Computer misuse. This includes breaking into other computers and spreading viruses. (Computer Misuse Act)***
- ***Ask permission from the holder if using copyrighted information. (Copyright, Designs, and Patents Act)***
- ***Please do not infringe other people's privacy. Ask before you publish someone's information over the Internet. (Data Protection Act)***

Users should also take care not to disrupt others. Please respect other users and members of staff.

We aim to allow for as much freedom of expression as possible. The library is also a public space. Take care accessing material as others may be able to see.

Service commitments

[NAME] cannot be held responsible in the event of loss of power. If you are having technical difficulties please speak to a member of staff. The Internet contains a vast amount of information. Some of this information may be inaccurate or illegal. [NAME] Library Service cannot be held responsible for information accessed. We ask that all users take care when surfing the Web. If you have any concerns please ask a member of staff.

User information will be treated with the strictest confidence. We will treat all user data under the Data Protection Act.

User commitments

If a user misuses the service or disrupts other users a warning will be given. If they continue to do so they may be asked to leave the premises. If this persists, they may be suspended for one month. After suspension, this will become a three month ban. Appeals can be made against these decisions. This can be done in person, or by telephone, email, or letter:

[Address]

Please accept this policy to continue