Public Library Quarterly

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/wplq20

Communicating Patron Rights and Responsibilities Transparently: Creating a Model Internet Acceptable Use Policy for UK Public Libraries

Elaine Robinson & David McMenemy

To cite this article: Elaine Robinson & David McMenemy (2022) Communicating Patron Rights and Responsibilities Transparently: Creating a Model Internet Acceptable Use Policy for UK Public Libraries, Public Library Quarterly, 41:4, 381-405, DOI: 10.1080/01616846.2021.1936883

To link to this article: https://doi.org/10.1080/01616846.2021.1936883

© 2021 The Author(s). Published with license by Taylor & Francis Group, LLC.

Published online: 07 Jul 2021.

Submit your article to this journal

Article views: 990

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=wplq20

PUBLIC LIBRARY QUARTERLY
2022, VOL. 41, NO. 4, 381–405
https://doi.org/10.1080/01616846.2021.1936883

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Communicating Patron Rights and Responsibilities Transparently: Creating a Model Internet Acceptable Use Policy for UK Public Libraries

Elaine Robinson and David McMenemy

Computer and Information Sciences, University of Strathclyde, Glasgow UK

ABSTRACT

Facilitating access to the Internet is an important part of the public library mission, and is crucial in ensuring that all citizens have the possibility of access to contemporary digital information and public services. Part of managing this access relies on the Acceptable Use Policy (AUP), an agreement between the library and the user regarding the conditions of access. This article reports on a national UK study of public library AUPs and the development of a new national model policy for public libraries, and which can be considered as 'best practice'. The article reports analysis of AUPs across the UK, with specific focus on how they communicate the use of filtering, and surveillance. This research adds new insight by studying the content of AUPs and contributes to the limited research that exists on public library AUPs in the UK. The research analyzed AUPs from 205 authorities in the UK, a return rate of 99.5%. The resulting conclusions and synthesis of relevant guidance on AUPs led to the formation of the model policy presented in this article.

ARTICLE HISTORY
Received July 2020
Accepted May 2021

KEYWORDS
Public libraries; acceptable use policy; qualitative content analysis; filtering; surveillance

Introduction

This paper explores the creation of a single Internet Acceptable Use Policy (AUP) that could be utilized by public libraries in the United Kingdom (UK). Public libraries in the UK are an important information source for citizens and help to foster digital inclusion and bridge the digital divide – in that they provide a crucial access point to online digital services. In doing so, libraries provide access to information about public services, opportunities to undertake online transactions (such as applying for permits and benefits) as well as opportunities to communicate with public service providers (by e-mail or other online forms). The digital divide is defined as "the gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard to both their opportunities to access information and communication technologies (ICTs) and to their use of the Internet for a wide variety of activities" (OECD 2001, 5).

CONTACT David McMenemy d.mcmenemy@strath.ac.uk Computer and Information Sciences, University of Strathclyde, Glasgow UK

© 2021 The Author(s). Published with license by Taylor & Francis Group, LLC.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Although 93% of households in the UK have Internet access that still leaves almost 2 million households without (ONS 2019a). As well as this, 7.5% of adults had not used the Internet by 2019 (ONS 2019b). By assisting patrons using the Internet and providing support for those learning digital skills by providing introductory Internet sessions, the library is a key part of facilitating digital inclusion and an important part of tackling the digital divide (DCMS 2017; OECD 2001). As well as providing access to ICT facilities for personal or academic use, the public library is also an important part of facilitating and educating on e-government services and digital citizenship. Digital citizenship is described as "the (self-)enactment of people's role in society through the use of digital technologies" (Hintz, Dencik, and Wahl-Jorgensen 2017, 731). With more focus on the use of e-government to deliver key services, the public library is vital for patrons who do not otherwise have access to the Internet, especially for those without access at home (Jaeger and Bertot 2009). The modern library provides a crucial community access point to digital services and information.

Research context

The key themes in this literature review that will be used to inform the analysis of the AUPs will, then, focus on (1) how surveillance and monitoring is communicated to users in the AUPs (2) how Internet filtering is communicated to users in the AUPs. The third key focus will utilize the literature on AUP best practice.

Managing access

Facilitating access to the Internet is an important part of the public library profession. The library is not in control of the Internet, and thus being able to manage this access by having certain policies and standards in place is particularly important, both for the library and its user base (ALA 2007b; Mcmenemy 2014; Pautz 2013). Key considerations here include preventing patrons from accessing material that might be illegal, or inappropriate for a public library setting. In addition, the policies and standards also communicate to patrons the categories of behavior that the public library expects from patrons, as well as protecting the library itself from any legal peril due to inappropriate use by a patron.

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. Access management in libraries includes surveillance, Internet filtering, and Acceptable Use Policies (AUPs).

Filtering

Filtering is a widely used method of access management (Brown and Mcmenemy 2013; Cooke et al. 2014; Payne 2016; Willson and Oulton 2000). Filtering software attempts to block or control content on the Internet that a user can access using a set of pre-defined criteria, including IP addresses, stopwords, and repositories of domain names (Shirazi 2012). In the library, filtering software is usually used 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). Filtering can protect users (Auld and Kranich 2005), and can reassure both patrons and staff (Heok and Luyt 2010; Spacey et al. 2014; Willson and Oulton 2000). 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 objectionable content is hidden from the patron.

The use of filtering however, is also contentious. One of the main arguments against filtering is that by denying patrons access to content, it is effectively a form of censorship (Mcmenemy and Burton 2005). Such practice goes against fundamental library ethics (Spacey et al. 2015). The argument that filtering is censorship is exacerbated by both its unreliability and the over-reliance 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 (ALA 2015; May 2014; Pautz 2013; Skaggs 2002; Stewart 2000; Wyatt 2006). Its lack of nuance has made filtering controversial (Poulter 2005). The use of filtering 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 (Gottschalk 2007; Kranich 2004; Pors 2001).

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). The Managing Access in Public Libraries (MAIPLE) project found that observation by both staff and monitoring software were popular methods of access management (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, Mcmenemy, and

Poulter 2015). Public libraries also use surveillance cameras for monitoring (Newell and Randall 2013).

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 also seen as a necessary tool for protection and as a detector of crime. Libraries must balance privacy issues with issues of public safety. 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 American Library Association (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 will expect the library to monitor them (Wyatt 2006).

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).

The acceptable use policy

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 was in place, or being developed (Willson and Oulton 2000). The MAIPLE project utilized 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, Mcmenemy, and Poulter 2015).

Summarizing what was seen to be best practice in the construction of the policy, Sturges suggests that AUPs should have seven essential features. These are set out in Table 1 below.

Table 1. AUP best practice.

Aims and Objectives	It is essential that the policy states the purpose of the service.
Eligibility	Who can use the service, including registration details and child access.
Scope	Service boundaries defining limitations.
Illegal Use	Sturges suggests that simply stating "no illegal use" is not helpful without giving some context.
Unacceptable Use	This may include accessing material that is legal, but could be offensive to others, or behaviors 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.

Adapted from: (Sturges 2002, 122–123).

While AUPs are essential documents for public libraries to produce, there is little evidence of any significant cooperation between library services in designing and implementing them. Whilst there is some guidance on writing AUPs for public libraries, in the UK each one is written at the specific 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 ALA recommends all libraries adopt a policy, and as well as reflecting the library's mission and being updated regularly, the AUP should emphasize freedom of access, as well as setting reasonable conditions for usage allowance and behavior (ALA 2007b, 2012). As an important legal document, it should also be made sure that it is publicized to library users (Mcmenemy 2014). The AUP is important for public libraries for a number of reasons. The British Educational Communications and Technology Agency (BECTA) states 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). 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 (Heok and Luyt 2010; Mcmenemy 2014; Rusk 2001). As well as protecting the library, the AUP is an important part of making sure that public access is safe (Huang 2007).

Despite its importance, AUPs are often inadequate (Stewart 2000). 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: "it can be inferred that the AUP has been designed to protect the host institution, rather than proactively educating the user" (Doherty, Anastasakis, and Fulford 2011, 208). 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 (Gallagher, Mcmenemy, and Poulter 2015). 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 analyzed, which

highlighted the communal nature of the library (Gallagher, Mcmenemy, and Poulter 2015). Höne and Eloff note that in professional organizations information security policies are seen by users as superfluous and pointless documents that are a waste of time and energy to read (Höne and Eloff 2002). This is exacerbated by policies that are not composed properly or regularly updated (Laughton 2008).

Despite the importance of the AUP, there is a lack of research on the public library AUP, particularly its content (Mcmenemy 2014). As part of the MAIPLE project, AUP documents were analyzed 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, Mcmenemy, and Poulter (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 analyze AUP content, length, and tone. Access management tools such as filtering have been studied using surveys and the Freedom of Information Act (such as Payne 2016; Spacey et al. 2014), however analyzing the use of filtering through the AUP document has only been done on a small scale. By analyzing the actual AUP document itself, how access management tools such as filtering and surveillance are used, and importantly, how they are communicated to patrons, this paper aids our understanding in how these important tools are being implemented in UK public library services, and what best practice can be gleaned to arrive at a universal solution.

Methodology

The methodology for this research incorporated the use of Freedom of Information requests made to all UK public library services to obtain their AUPs, followed by qualitative content analysis of the AUPs based on the best practice literature on AUP design, and the literature on surveillance and monitoring, and filtering.

Data collection

In the UK there are 206 Public Library Authorities (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, AUPs were to be analyzed from every PLA. Each PLA usually creates its own AUP, meaning an AUP in one area of the UK will not be identical to another. To collect the AUPs, a combination of Internet searching and Freedom of Information (FOI) requests were used. FOI 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). They are enshrined in law as a mechanism for citizens to get access to public service information.

The FOI request sent to authorities stated:

> 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]

A total of 205 out of a possible 206 policies was collected, a return rate of 99.5%. Where FOI requests were necessary, they were sent either by e-mail or via webform depending on the options made available on local authority websites to make a request. The average reply was received in 14 days, some were sent the very same day, others took over two months (about 10%), due to mistaken e-mail addresses or clarification being required. AUPs were received by e-mail in various file formats as PDFs, Microsoft Word documents, Notepad documents, and image files.

Qualitative content analysis

The AUPs were analyzed using qualitative content analysis, 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 and Kyngäs 2008; Vaismoradi, Turunen, and Bondas 2013). 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 is particularly suited for documents such as the AUP for it can give insights into an individual or an organization's attitudes, values, and prejudices (Krippendorff 1989, 404). The stages of qualitative content analysis carried out for this study are based on Zhang and Wildemuth (2016, 318–330).

Step 1: preparation of data

In this case, deciding which texts were to be used for analysis was relatively straightforward. 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. The researchers managed to gather 205 out of a possible 206. Because of the data types used, documents, preparing the data for analysis was straightforward. Texts were imported into NVivo for analysis. As mentioned earlier, 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.

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. The themes that were defined from the literature review were surveillance and monitoring, including the subsets of monitoring care and monitoring control. In addition, the framework of best practice for AUPs defined by Sturges was also used as a primary tool of analysis.

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 Table 2. For space reasons not all codes explored are discussed in this paper.

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. 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 randomization.

Step 5: code the text

Once the pilot study was complete, the researchers carried out coding on all of the AUPs. 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.

Table 2. Guide to themes used in coding.

Theme: Surveillance and monitoring		
Sub-Category	Definition and Coding Rules	Example from AUPs
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.
Not Monitoring	Monitoring is explicitly not used	[NAME REMOVED] does not monitor your e-mail or other communications electronically
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 behavior will not be tolerated. Any individual or group who displays such behavior will be asked to leave
Illegal Use	Illegal usage of facilities	The Telecommunications Act 1984 makes it an offense 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

(*Continued*)

Table 2. (Continued).

Theme: Surveillance and monitoring		
Sub-Category	Definition and Coding Rules	Example from AUPs
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 leveled	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 nontransparent – 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 block all websites or erroneously block websites	The internet service is filtered in order to block access to websites known 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

Step 6: checking the coding

This step allows for the researchers 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 researchers 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.

Results and discussion

Although both the tone and content of the policies varied, there were some aspects that were covered in all of the AUPs. For example, almost all of the AUPs made some form of reference to illegal or unacceptable use of the facilities, as well as references to upholding or concern for the public good, discussion of service and user commitments, and outlining user commitments. The AUPs varied in length, ranging between 100 and almost 4,000 words, with the average word count being 817.

Surveillance and monitoring

Surveillance in the public library is carried out both physically by library staff, and electronically through the monitoring of e-mail and browsing habits. Monitoring as expressed in the AUPs varied to a large degree between library services. Some AUPs detailed their use of monitoring in a very explicit and transparent way. For example:

> 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)

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

> 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)

> The Council reserves the right to monitor and log all types of activity across the service. The Council will however endeavour to respect users' right to privacy at all times (AUP 60)

When discussing children's usage, a number of AUPs note that the library is not responsible for what they access; monitoring is something that is to provided by the caregiver.

Monitoring control

Monitoring control was referenced in 119 of the AUPs, with 143 references overall. Information was coded as monitoring control if the surveillance being carried out was specifically for regulatory or disciplinary purposes. Monitoring was used by staff to check if patrons were misusing the facilities, and to ensure library users were using facilities for what the library deemed as appropriate use or correct purpose. Often monitoring was not carried out for safety reasons, rather, surveillance was being used for checking up on user behavior. 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. At times, the monitoring seemed invasive:

> *"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."*

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:

> *"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."*

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 behavior. Certain elements of the AUPs evoked elements of Bentham's 'Panopticon' (Bentham and Bowring 1843). Some AUPs had taken care to make sure its users understand that their session is being monitored both in real time and after the fact. 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. This uncertainty is a key part of panopticism (Foucault 1991). 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.

Monitoring care

Some monitoring was used directly for the safeguarding of the patrons using the facilities. 35 AUPs were coded under monitoring care, with 40 references overall. Some AUPs directly stated that monitoring was for the safety of patrons. A number of the AUPs highlighted that the library was a shared space and so monitoring was necessary. Monitoring was also used to help support the library service:

> *"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."*

Most AUPs simply stated that monitoring was being used to "plan better services". 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. Transparency and clarity for the user is key: only 44 of the AUPs mention patron data is used and stored in compliance with the Data Protection Act.

Filtering

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 and 32 sources made no reference to filtering or blocking software.

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. Filtering software is characterized as having different uses in the AUPs: it safeguards patrons; it prevents material being exposed to patrons; it regulates usage; it blocks websites; and it bars users from accessing certain websites. Filtering is used as a defense 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. Some of the AUPs used the idea of mitigating against a risk or using filtering as a shield to protect users. Other AUPs emphasized the communal nature of the library. 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 behavior.

The view that the use of filtering software is a controlling mechanism was echoed in a number of the AUPs. Four AUPs use the word "suppress" to describe how filtering software operates. Some AUPs framed filtering as a response to bad behavior, rather than being a preventative measure:

> *"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."*

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 were the AUPs that gave no reason for filtering at all. 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.

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 remaining AUPs, 32 made no reference to filtering at all. Studies by the MAIPLE project (Spacey et al. 2014, 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. 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.

Efficacy of filtering and unblocking websites

Filtering 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. Of the 167 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.

The idea of checks was reflected in several of the AUPs. The use of words such as "investigation", "careful consideration", and "checking", evokes subtle gatekeeping and power by the library service. Some of the AUPs noted that personal tastes vary but encourage users to inform staff if they feel a website

has been wrongly categorized. Other AUPs state that patrons should "recommend" whether websites should be made accessible, which suggests a communal, shared library service.

> "*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.*"

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. 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. 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. The librarian cannot carry out their duty effectively if they are prevented from making the decisions themselves.

Filtering can both encourage and discourage information access. The AUPs analyzed 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.

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.

As well as general methods of access management such as filtering and surveillance, the AUPs were also analyzed for presence of commitment to the ethical principles of the information profession. Ethical principles are an important part of the information profession and the library service, as they govern important tenets such as freedom of access and expression, as well as concern for the public good and equitable treatment of information users. Some measures of access management such as filtering and surveillance can

come into conflict with the ethical principles of the information profession in the UK.

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 access management. Access to information was often encouraged as a goal, but at the same time discouraged through authoritarian language, 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 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 tended to overly rely on controlling ways of describing surveillance, with over half of the AUPs featuring the monitoring control node. Despite this, there was also aspects of caring and protective surveillance, although this was by a far fewer number of the AUPs.

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. 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.

Toward a model policy

The new national policy presented in this article (Appendix A) is based on Sturges' essential elements of an AUP (see Table 1 and Sturges 2002), combined with best practice as observed through the literature, and the evidenced empirical findings of this national study, including from from the qualitative content analysis. This policy is presented as providing a clear, understandable AUP that could be utilized across the UK public library sector.

Sturges states that an AUP should have seven key elements: aims and objectives; eligibility; scope; illegal use; unacceptable use; service commitments and user commitments. Alongside this, the AUP should have clarity and be direct in its approach, which will instill confidence in patrons and staff alike,

and should avoid vague and unnecessarily complicated wording, which will inhibit understanding and consequently make the document weaker.

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 noted by previous studies, there is both a lack of awareness and an apathy toward the AUP (Höne and Eloff 2002; Laughton 2008; McMenemy, 2008; Poulter et al. 2009; Doherty, Anastasakis, and Fulford 2011; Spacey et al. 2014). Having a document that is easily read is paramount to this process. The model policy was put through readability testing using the readability calculators on readable.io (previously readability-score.com). 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 final version, provided as Appendix 1 scored as follows:

- Flesch Reading Ease: 66.7
- SMOG Grade: 9.4
- Gunning Fog Index: 8.0
- Coleman-Liau Index: 8.0

Elements of the policy

The proposed new national model policy contains six main sections, and includes a number of elements, which cover its purpose, coverage and functionality. The model policy is primarily based on Sturges (2002), as well as best practice guidance from the literature review, and the findings from the qualitative content analysis. Our key difference from Sturges' six categories is that we combined "illegal use" and "unacceptable use" into one single category, "misuse". In our view this streamlined the document and also allowed us to focus less on negative, legalistic language and more on patron expectations. Table 3 summarizes the sections of the model policy.

Welcome section

Of the 205 AUPs analyzed, 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. 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 (Kelehear 2005; Palgi 1996; Pautz 2013; Scott and Voss 1994). 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 researchers 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. Communicating to the patron the values of the service and the purpose of it is an excellent way to focus the welcome statement, and we therefore saw the inclusion of a welcome statement was a key way of communicating with the patron is a friendly and informative way.

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 analyzed 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.

Scope of service and filtering information

It is important to state what the limits of the service are, and whether this includes personal use (McMenemy 2009; Sturges 2002). As noted by a number of guidelines, explanations should be clear, avoiding too much

Table 3. National AUP model policy sections summary.

Welcome	An introduction to the AUP, explaining why it has been created and what the aims of the service are
Eligibility	Who can use the service
Scope of service and filtering information	What the limits of the service are. Explain the use of filtering clearly
Misuse	Define what constitutes as misuse of the service
Service commitments	Outline the responsibilities of the service to the patron
User commitments	Outline what the library expects of the patron

jargon (e.g. ALA 2007b; Höne and Eloff 2002; Palgi 1996; Pautz 2013; Scott and Voss 1994; Sturges 2002). 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. It was also important to ensure users knew what to do in the case of the filtering software being in error. 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.

Misuse

Defining what constitutes as misuse and illegal use is a key part of any AUP (ALA 2007b; Kelehear 2005; Laughton 2008; Scott and Voss 1994; Sturges 2002). The findings from Gallagher, McMenemy, and Poulter (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.

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.

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.

Concluding comments

This study has found public library AUPs to be very varied and inconsistent, with examples of both good and bad practice throughout. The differences between each document indicate that access is not uniform for public library visitors across the UK. There is no reason why the UK should not have a single AUP which would ensure uniform and fair access. A public library service should not change across different parts of the country and access to the digital services and information should not be variable according to postcode. 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. Access should be equal and a single, robust national standard AUP would reflect this.

The public library is an important hub for internet access for citizens and provides a key forum for engagement with the government and the use of e-government services. It is also an important venue for fostering digital citizenship which requires "regular and effective Internet access and the skills to use the technology" (Mossberger, Tolbert, and Hamilton 2012, 2493). The AUP is an important part of managing this access, and the AUP document can be used to inform the patron of good Internet use, as well as imparting the principles of digital citizenship (Robinson and McMenemy 2019). In many ways, the library AUP provides a 'gateway' to digital services and information, and should not be underestimated as it plays a pivotal role in strategies and practices designed to bridge the digital divide.

To keep up with the advancements in new digital online technologies the AUP has seen an evolution in how librarianship is practiced, including new measures that represent a move toward using technology to try and improve the library service, but also perhaps a move toward the surveillance society. The national standardized AUP policy proposed in this article can act as a model for which new AUPs are based, thus ensuring a more uniform service, as well as paying attention to the important parts of library service, including adhering to users' privacy and information access rights, as well as reflecting the ethical principles of the profession.

Funding

This work was supported by the Economic and Social Research Council [ES/J500136/1].

Notes on contributors

Dr Robinson recently completed her PhD at the University of Strathclyde, and is a Research Associate in the Department of Computer and Information Sciences. She has also worked as a Research Associate at the Universities of Stirling, and Dundee. Her research focuses on the impacts of technology on citizens, and she has experience of both qualitative and quantitative methodologies.Dr McMenemy is a Senior Lecturer in the Department of Computer and Information Sciences at the University of Strathclyde, and has an extensive publication record and experience in the fields of public libraries and digital ethics, authoring two books on modern public libraries, and numerous research articles on public library digital services and how they can be ethically managed.

Dr McMenemy is a Senior Lecturer inthe Department of Computer and Information Sciences at the University of Strathclyde, and has an extensive publication record and experience in the fields of public libraries and digital ethics, authoring two books on modern public libraries, and numerous research articles on public library digital services and how they can be ethically managed.

References

ALA. 2007a. Questions and answers on privacy and confidentiality. [Online]. http://www.ala.org/advocacy/privacy/FAQ Last accessed: 30th June 2020

ALA. 2007b. Libraries and the Internet Toolkit: Internet Policies. [Online]. http://www.ala.org/advocacy/intfreedom/iftoolkits/litoolkit/internetusepolicies Last accessed: 30th June 2020

ALA. 2012. Libraries and the internet toolkit: tips and guidance for managing and communicating about the Internet. [Online]. http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/intfreedom/iftoolkits/litoolkit/2012internettoolkit.pdf Last accessed: 30th June 2020

ALA. 2015. Internet filtering. [Online]. http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/internet-filtering Last accessed: 30th June 2020

Auld, H., and N. Kranich. 2005. Do internet filters infringe upon access to material in libraries? *Public Libraries* 44 (4):196–204.

BECTA. 2009. AUPs in context: Establishing safe and responsible online behaviours [Online]. http://www.wisekids.org.uk/BECTA%20Publications/aups_context_online_behaviours.pdf Last accessed: 30th June 2020

Bentham, J., and J. Bowring. 1843. The works of Jeremy Bentham. vol. 4 (Panopticon, Constitution, Colonies, Codification). Edinburgh: W. Tait. [Online]. https://oll.libertyfund.org/titles/1920

Brown, G. T., and D. McMenemy. 2013. The implementation of internet filtering in Scottish public libraries. *Aslib Proceedings* 65 (2):182–202. doi:10.1108/00012531311313998.

Bryman, A., 2012. *Social research methods*4th ed., Oxford: Oxford University Press

CILIP. 2011. User privacy in libraries: Guidelines for the reflective practitioner [Online]. https://www.cilip.org.uk/sites/default/files/documents/Privacy_June_AW.pdf Last accessed: 30th June 2020

CILIP. 2015. *Libraries and information services in the United Kingdom and the Republic of Ireland 2015*. London: Facet.

Cooke, L. 2006. Do we want a perfectly filtered world? (Guest editorial). *Library Student Journal*, 2. [Online]. htttp://www.librarystudentjournal.org/index.php/lsj/article/view/21/162

Cooke, L., R. Spacey, C. Creaser, and A. Muir. 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):5–19. doi:10.29173/lirg620.

DCMS. 2017. UK digital strategy 2017 [Online]. https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy Last accessed: 30th June 2020

Doherty, N. F., L. Anastasakis, and H. Fulford. 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):201–09. doi:10.1016/j.ijinfomgt.2010.06.001.

Elo, S., and H. Kyngäs. 2008. The qualitative content analysis process. *Journal of Advanced Nursing* 62 (1):107–15. doi:10.1111/j.1365-2648.2007.04569.x.

Foucault, M. 1991. *Discipline and punish: The Birth of the prison*. London: Penguin.

Gallagher, C., D. McMenemy, and A. Poulter. 2015. Management of acceptable use of computing facilities in the public library: Avoiding a panoptic gaze? *Journal of Documentation* 71 (3):572–90. doi:10.1108/JD-04-2014-0061.

Gottschalk, L. 2007. Internet filters in public libraries: Do they belong? *Library Student Journal* Retrieved from www.librarystudentjournal.org/index.php/lsj/article/view/25/17 . Last accessed: 30th June 2020

Heok, A., and B. Luyt. 2010. Imagining the internet: Learning and access to information in Singapore's public libraries. *Journal of Documentation* 66 (4):475–90. doi:10.1108/00220411011052911.

Hintz, A., L. Dencik, and K. Wahl-Jorgensen. 2017. Digital citizenship and surveillance society. *International Journal of Communication* 11:731–39.

Höne, K., and J. H. P. Eloff. 2002. What makes an effective information security policy? *Network Security* 2002 (6):14–16. doi:10.1016/S1353-4858(02)06011-7.

Hsieh, H.-F., and E. Shannon. 2005. Three approaches to qualitative content analysis. *Qualitative Health Research* 15 (9):1277–88. doi:10.1177/1049732305276687.

Huang, P. 2007. How you can protect public access computers. *Computers in Libraries* 27 (5):16–20.

Jaeger, P. T., and J. C. Bertot. 2009. E-government education in public libraries: New service roles and expanding social responsibilities. *Journal of Education for Library and Information Science* 50 (1):39–49.

Kelehear, Z. 2005. When email goes bad: Be sure that your AUP cover staff as well as students. *American School Board Journal*. 32–34. v192 n1 January 2005

Kline, M. 1999. Mainstream Loudoun v. Board of trustees of the Loudoun county library. *Berkeley Technology Law Journal* 14 (1):347–70.

Kranich, N. 2004. Why filters won't protect children or adults. *Library Leadership & Management* 18 (1):14.

Krippendorff, K. 1989. Content analysis. In *International encyclopedia of communication*, ed. E. Barnouw, G. Gerbner, W. Schramm, T. L. Worth, and L. Gross. Oxford: Oxford University Press. pp. 403-407

Laughton, P. 2008. Hierarchical analysis of acceptable use policies. *South African Journal of Information Management* 10 (4):2–6.

May, J. 2014, January 27. What's the best way to keep children safe online? [CILIP Blog]. https://archive.cilip.org.uk/blog/what-s-best-way-keep-children-safe-online Last accessed: 30th June 2020

McMenemy, D., and P. F. Burton. 2005. Managing access: Legal policy and issues of ICT use. In *Delivering digital services: A handbook for public libraries and learning centres*, ed. D. McMenemy and A. Poulter, 156–175). London: Facet.

McMenemy, D. (2008). Internet access in UK public libraries: Notes and queries from a small scale study: Editorial. *Library Review*, 57(7), 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.
Mossberger, K., C. J. Tolbert, and A. Hamilton. 2012. Measuring digital citizenship: Mobile access and broadband. *International Journal of Communications* 6:2492–528.
Newell, B. C., and D. P. Randall. 2013. Video surveillance in public libraries: A case of unintended consequences? In System Sciences (HICSS), 2013 46th Hawaii International Conference on System Sciences, Wailea, Maui, HI USA, IEEE, 1932–41.
OECD. 2001. Understanding the Digital Divide [Online]. http://www.oecd.org/dataoecd/38/57/1888451.pdf Last accessed: 30th June 2020
ONS. 2019a. Internet access – Households and individuals, Great Britain: 2019 [Online]. https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2019 Last accessed: 30th June 2020
ONS. 2019b. Internet users, UK: 2019 [Online]. https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2019 Last accessed: 30th June 2020
Palgi, R. D. 1996. Rules of the road: Why you need an acceptable use policy. *School Library Journal* 42 (8):32–33.
Pautz, H. 2013. Managing access to the internet in public libraries. *New Library World* 114 (7/8):308–18. doi:10.1108/NLW-01-2013-0007.
Payne, D. 2016. New research maps the extent of web filtering in public libraries. [Online]. http://www.cilip.org.uk/blog/new-research-maps-extent-web-filtering-public-libraries Last accessed: 30th June 2020
Pors, N. O. 2001. Misbehaviour in the public library: Internet use, filters and difficult people. *New Library World* 102 (9):309–13. doi:10.1108/EUM0000000005899.
Poulter, A. 2005. *The library and information professional's internet companion: A practical resource for library and information professionals*. London: Facet.
Poulter, A., I. Ferguson, D. McMenemy, and R. J. Glassey. 2009. Question: Where would you go to escape detection if you wanted to do something illegal on the internet? Hint: Shush! In *Global security, safety and sustainability: 5th international conference, ICGS3. Communications in computer and information science (1st)*, ed. H. H. JAHANKHANI and F. HSU. London: Springer-Verlag. pp.1-8.
Robinson, E., and D. McMenemy. 2019. 'To be understood as to understand': A readability analysis of public library acceptable use policies. *Journal of Librarianship and Information Science* 52 (3):713–25. doi:10.1177/0961000619871598.
Rusk, M. 2001. Acceptable use policies: Four examples from community college libraries. *Community & Junior College Libraries* 10 (2):83–90. doi:10.1300/J107v10n02_10.
Savage, A., and R. Hyde. 2014. Using freedom of information requests to facilitate research. *International Journal of Social Research Methodology* 17 (3):303–17. doi:10.1080/13645579.2012.742280.
Scales, P. 2009. Better safe than sorry: Does your library have an online acceptable-use policy? *School Library Journal* 55 (3):22.
Scott, T. J., and R. B. Voss. 1994. Ethics and the 7 "P's" of computer use policies. ECA 1994 Proceedings of the Conference on Ethics in the Computer Age, Galtinburg Tennessee USA. 61–67.
Shirazi, F. 2012. Free and open source software versus Internet content filtering and censorship: A case study. *Journal of Systems and Software* 85 (4):920–31. doi:10.1016/j.jss.2011.11.1007.
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):809–52.

Spacey, R., L. Cooke, C. Creaser, and A. Muir. 2014. *Managing access to the internet in public libraries [MAIPLE]. loughborough*. Leicestershire: LISU. https://www.lboro.ac.uk/microsites/infosci/lisu/maiple/downloads/maiple-report.pdf Last accessed: 30th June 2020

Spacey, R., L. Cooke, C. Creaser, and A. Muir. 2015. Regulating internet access and content in UK public libraries: Findings from the MAIPLE project. *Journal of Librarianship and Information Science* 47 (1):71–84. doi:10.1177/0961000613500688.

Stewart, F. 2000. Internet acceptable use policies: Navigating the management, legal, and technical issues. *Information Systems Security* 9 (3):1–7. doi:10.1201/1086/43310.9.3.20000708/31360.6.

Sturges, R. P. 2002. *Public internet access in libraries and information services*. London: Facet.

Vaismoradi, M., H. Turunen, and T. Bondas. 2013. Qualitative descriptive study. *Nursing & Health Sciences* 15:398–405. doi:10.1111/nhs.12048.

Willson, J., and T. Oulton. 2000. Controlling access to the internet in UK public libraries. *OCLC Systems & Services: International Digital Library Perspectives* 16 (4):194–201. doi:10.1108/10650750010354166.

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):70–79. doi:10.3172/JIE.15.1.70.

Zhang, Y., and B. M. Wildemuth. 2016. Qualitative analysis of content. In *Applications of social research methods to questions in information and library science*, B. A. Wildmuth ed., 2nd ed., Oxford: Pearson Education.

Appendix A. 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*
- *E-Mail 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. E-Mail 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 e-mail, 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. If you would like more information on how your information is stored please contact staff in person, or by telephone, e-mail, or letter.

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, e-mail, or letter:

[Address]

Please accept this policy to continue.