Athens Institute for Education and Research
ATINER

ATINER's Conference Paper Series
LIB2014-1679

Managing Access to the Internet in Public Libraries in the UK – The Findings of the MAIPLE Project

Rachel Spacey
Researcher
Loughborough University
UK

Louise Cooke
Loughborough University
UK

Claire Creaser
Loughborough University

Adrienne Muir
Loughborough University
UK

An Introduction to ATINER's Conference Paper Series

This paper should be cited as follows:

Spacey, R., Cooke, L., Creaser, C., and Muir, A. (2015). **"Managing Access to the Internet in Public Libraries in the UK ‑ The Findings of the MAIPLE Project",** Athens: ATINER'S Conference Paper Series, No: **LIB2014-1679.**

Athens Institute for Education and Research
8 Valaoritou Street, Kolonaki, 10671 Athens, Greece
Tel: + 30 210 3634210 Fax: + 30 210 3634209 Email: info@atiner.gr URL: www.atiner.gr
URL Conference Papers Series: www.atiner.gr/papers.htm
Printed in Athens, Greece by the Athens Institute for Education and Research. All rights reserved. Reproduction is allowed for non-commercial purposes if the source is fully acknowledged.
ISSN: 2241-2891
4/11/2015

Managing Access to the Internet in Public Libraries in the UK - The Findings of the MAIPLE Project

Rachel Spacey
Louise Cooke
Claire Creaser
Adrienne Muir

Abstract

One of the key purposes of the public library is to provide access to information[1]. In the UK, information is provided in printed formats and for the last decade via public access Internet workstations installed as part of the People's Network initiative. Recent figures reveal that UK public libraries provide approximately 43,000 computer terminals offering users around 83,000,000 hours across more than 4,300 service points[2]. In addition, increasing numbers of public libraries allow users to connect devices such as tablets or smart phones to the Internet via a wireless network access point (Wi-Fi). How do public library staff manage this? What about users viewing harmful or illegal content? What are the implications for a profession committed to freedom of access to information and opposition to censorship?

MAIPLE, a two-year project funded by the Arts and Humanities Research Council (AHRC) has been investigating this issue, as little was known about how UK public libraries manage Internet content control including illegal material. MAIPLE has drawn on an extensive review of the literature, an online survey which all UK public library services (PLS) were invited to complete (39 per cent response rate) and case studies with five services (two in England, one in Scotland, one in Wales and one in Northern Ireland) to examine the ways these issues are managed and their implications for staff.

This paper will explore the prevalence of tools such as filtering software, Acceptable Use Policies (AUPs), user authentication, booking software and visual monitoring by staff and consider their efficacy and desirability in the provision of public Internet access. It will consider the professional dilemmas inherent with managing content and access. Finally, it will highlight some of the more important themes emerging from the findings and their implications for practitioners and policy makers.

Keywords: Public libraries, Internet, Filtering

Acknowledgements: The authors would like to thank the members of the External Advisory Board, 'critical friends' and all the public library staff and Internet users who took part in the project. The work of Sharon Fletcher and Sonya White in LISU is also appreciated. This project was supported by the Arts and Humanities Research Council (AHRC) [grant number AH/J005878/1].

[1] UNESCO (1994). *UNESCO Public Library Manifesto*. Available at: http://www.unesco.org/webworld/libraries/manifestos/libraman.html

[2] CIPFA (2013) *Public library statistics. 2013-2014 Estimates and 2012-2013 Actuals*. London: The Chartered Institute of Public Finance and Accountancy.

Introduction

In the UK, public libraries provide access to the Internet on PCs as well as an increasing number of libraries which provide Wi-Fi access. In the majority of services, but not all, Internet access via these two means is free[3]. This paper considers how public libraries manage acceptable use of the Internet using a range of tools including AUPs, content filtering software, booking systems, user authentication and visual monitoring. The paper is based on the findings of the AHRC funded MAIPLE project (September 2012 - August 2014). It provides contextual background and details the methods used in the study. Selected findings are considered here and their implications for staff, the public library profession and policy makers, discussed.

Background

Public libraries in the UK were the beneficiaries of a £100 million scheme launched in 2000 - the People's Network (PN) funded by the New Opportunities Fund (NOF), a National Lottery good cause distributor for health, education, and the environment, public libraries in the UK (England, Scotland, Wales and Northern Ireland). The project aimed to connect every public library to the Internet by the end of 2002. To complement this roll out of ICT infrastructure, in late 1999, a £20 million ICT training programme for public library staff commenced which was also funded by NOF. A staggering "*30,000 computer terminals in over 4,000 libraries, providing broadband internet access and a suite of software*"[4] were rolled out across the UK. The most recent publicly available statistics from 2013[5] reveal that there are now almost 43,000 computer terminals providing library users with a potential 83,430,527 hours of Internet access per annum across the 206 PLS in the UK of which 32,839,424 were recorded as used (39 per cent). Of the 4,313 public library service points across the UK, 1,553 (36 per cent) provide public access Wi-Fi.

Since its arrival, the Internet has been a popular service offering members of the public the opportunity to communicate by email, engage with government services online, search for information and use social media such that by 2009 it was observed that: "*the Internet is now both integral and*

[3] In 2013, Internet access was free to library members in 111 authorities in England and Wales whilst 47 authorities imposed a charge only after an initial free period, which varied from 30 minutes to four hours. A total of 38 authorities provided details on Wi-Fi access, with 36 indicating that it is free to library members, with a further two authorities stating that they impose a charge only after an initial free period (LISU, 2013).

[4] Hardie-Boys, N. (2004). *The People's Network: evaluation summary*. London: Big Lottery Fund. Available at: http://www.biglotteryfund.org.uk/er_eval_peoples_network_ evaluation _summary_uk.pdf

[5] CIPFA (2013). *Public library statistics. 2013-2014 Estimates and 2012-2013 Actuals*. London: The Chartered Institute of Public Finance and Accountancy.

essential to the purpose of libraries in providing access to e-government, information, learning and community cohesion" (MLA, 2009, p. 13). However, concern has been voiced about the potential the Internet provides to library users wishing to view illegal content and/or "*access offensive material*" (Spacey, 2003, p. 28).

In the UK illegal material includes sites with images of child sexual abuse or which incite racial or religious hatred and/or violence. Material which is offensive is much harder to define since offensiveness is subjective and is what upsets or disgusts others but it may include pornography, for example. In addition, there are copyright laws which public libraries must adhere to. Misuse could include using peer-to-peer technology to download music illegally. There is certainly evidence internationally, that since the Internet was introduced into public libraries a minority of users have accessed material which is illegal or offensive (see, for example, Pors 2001; Ward 2003; Cavanagh 2004; Sommerlad et al., 2004; Comer 2005; Poulter et al., 2009; Australian Library and Information Association 2011).

In the early years of the PN it was not clear how public libraries were managing misuse such as users viewing illegal and/or offensive materials online. One early PN evaluation report found that approximately three quarters of 41 per cent responding services had installed filtering software which equated to approximately 60 of 210 services (Brophy, 2003). This scarcity of data informed the development of the MAIPLE project which aimed to ascertain just how widely PLS used filtering software and what other techniques and tools were being utilised to manage acceptable access.

Methods

In order to gauge what was happening in UK PLS, an in-depth literature review was undertaken which considered the history of Internet access in public libraries in the UK as well as research relating to the management of Internet access in public libraries worldwide. Research exploring examples of misuse and organisational measures to manage Internet use were also examined (see Spacey et al., 2014a). This informed the creation of an online survey which one senior manager in every UK PLS was invited to complete, with a response rate of 39 per cent (see Spacey et al., 2014b). To further examine the findings of the survey, five case studies were authored based on visits to five services. Case study methods included interviews with staff at varying organisational levels, and Internet users supported by observation and documentary analysis. A further piece of desk research was undertaken to provide information about public Wi-Fi developments in the UK affecting commercial outlets such as coffee shops and restaurants with which to contextualise the five PLS case studies.

Selected Findings

The results of the online MAIPLE survey undertaken in February 2013 revealed that all 80 responding UK PLS provided filtered access to the Internet on all their PCs (100.0 per cent). Two-fifths of respondents used Websense filtering software (40.0 per cent). The second most popular filtering package, used by nine services, was Blue Coat (11.3 per cent). Of the 67 responding services that provided Wi-Fi, the majority, *n*=56, provided filtered wireless Internet access (83.6 per cent); eight services provided unfiltered Wi-Fi (11.9 per cent) and three respondents did not know. Over half of responding services provided secure Wi-Fi access either Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access II (WPA2) (*n*=40, 59.7 per cent), the two security protocols and security certification programs developed to secure wireless computer networks. One-quarter of respondents did not know (*n*=17, 25.4 per cent) if their Wi-Fi access was secure and ten services provided unsecured access (14.9 per cent).

Almost all of the responding services had an AUP for public Internet usage, *n*=79 (98.8 per cent). One respondent did not know. In terms of what library members and non-members (guests) needed in order to access the Internet in their libraries, almost all services required members to have a borrower number (98.8 per cent) and in 70 services, a PIN or password was also required (87.5 per cent). For guests, half of responding services required some proof of identity (50.0 per cent) whilst a PIN or password was required by almost half of responding services (47.1 per cent). A quarter of responding services required a means of payment (25.0 per cent). In five services, no user authentication was required (7.4 per cent).

The most commonly used measure, after filtering software and AUPs, to manage public Internet access was visual monitoring by library staff (83.5 per cent). The location of PCs and use of a booking system were also popularly used methods (70.9 per cent). Over 90 per cent of responding services (*n*=73) used a proprietary software booking or reservation system giving users the opportunity to reserve a time-slot on a library PC (92.4 per cent). The most widely used reservation system was Netloan by Lorensbergs (54.8 per cent) while almost one-third used i-CAM by Insight Media Internet Limited. Over two-fifths of respondents (44.3 per cent) collected Internet use data. Monitoring software was used by almost a third of responding services (30.4 per cent).

In terms of the effectiveness of these different tools and approaches in managing Internet use, over half of all respondents judged filtering to be ‘very useful’ (*n*=45, 56.3 per cent) and approximately two-fifths found it ‘somewhat useful’ (*n*=33, 41.3 per cent). Only two respondents judged it to be ‘not very useful’ (2.5 per cent). Overall, filtering software and an electronic booking system for Internet use emerged as the most popular options to manage Internet access. However, in spite of the range of measures in place to manage Internet access, misuse was still recorded. Roughly two-fifths of respondents thought that library users sometimes circumvented the Internet filter (*n*=33, 41.3 per cent) although around one-third perceived that it rarely happened (*n*=27, 33.8 per cent). Around one-fifth of respondents did not know (n=17, 21.3 per cent) and three thought that it never happened (3.8 per cent). No respondents thought it was a frequent problem. 'Major' breaches of the AUP were known to occur 'rarely' (*n*=30, 38.0 per cent) and 'sometimes' (*n*=25, 31.6 per cent) in the majority of responding authorities. According to 10 respondents, breaches 'never' happen (12.7 per cent) whilst in 14 services, the respondent did not know (17.7 per cent). 'Major' breaches of the AUP were generally considered to be the result of library users viewing obscene (legal and illegal) content (82.2 per cent). Viewing racist, extremist or hate content as a 'major' breach of the AUP was noted in six services (13.3%) whilst in fewer than 10 per cent of responding services' 'major' AUP breaches involved hacking (8.9 per cent), criminal activity (4.4 per cent) or spamming (1.8 per cent). 'Other' 'major' breaches (four) included damage to equipment, users attempting to log-in with other users' details and inappropriate user behaviour. Misuse incidents involving minors rarely happened according to approximately two-fifths of respondents (43.8 per cent). It was reported by 30 per cent of respondents that such incidents never happened (*n*=24) whilst in 12.5 per cent of responding services, they sometimes happened (*n*=10). Eleven respondents did not know.

Survey respondents were asked about objections from library users in relation to filtering. Almost two-thirds of survey respondents had received complaints (n=52, 65.8 per cent) from library users about the filtering software in the last 12 months of which over-blocking was the most frequent cause (88.5 per cent) whilst the inability to upload or share files was also cited by over half of respondents receiving complaints (53.8 per cent). In most of the services we questioned, library users can request a change in the filtering policy by asking a member of staff in the library (76.3 per cent) or by emailing a request to the library service (50.0 per cent). Approximately one-fifth of services give users the opportunity to complete a request form online (21.3 per cent) or complete a paper form in the library (22.5 per cent).

Discussion

Filtering software, also known as content-control software, content filtering software, censorware, content-censoring software, web filtering software or content-blocking software are all terms used to describe software designed to control or restrict access to content online or software that blocks access to certain websites. It may be installed on individual computers but in public libraries is usually done on a network basis. The use of filtering software is frequently justified on moral grounds as a way in which to protect children from the unsavoury aspects of the Internet such as sexual content (Byron, 2008). In addition, it has been suggested that public library staff find dealing with users viewing offensive or illegal content distressing (Poulter et al., 2009) and filtering can help alleviate this unpleasant aspect of the role (Sturges, 2002).

However, the use of filtering software is controversial not least because of its technical limitations. Filtering can lead to over-blocking and under-blocking of content and filters may be bypassed. As the MAIPLE survey results reveal, library staff reported misuse incidents in spite of filtering software and complaints from users were usually because the filter blocked content they considered legitimate.

Moreover, in spite of the inconveniences for users in terms of finding sites blocked or having to ask to have a site unblocked, there are wider, professional and ethical issues at stake. According to the International Federation of Library Associations (IFLA), "*In more than 60 countries library associations have developed and approved a national code of ethics for librarians*" (IFLA, 2014) and in 2012, IFLA itself endorsed the *IFLA Code of Ethics for Librarians and Other Information Workers* (IFLA, 2012). The code has six sections: access to information; responsibilities towards individuals and society; privacy, secrecy and transparency; open access and intellectual property; neutrality, integrity and personal skills; and colleague and employer/employee relationship. This "*series of ethical propositions*" states: "*Librarians and other information workers reject the denial and restriction of access to information and ideas most particularly through censorship whether by states, governments, or religious or civil society institutions*" (IFLA, 2012). In the UK, the Chartered Institute of Library and Information Professionals (CILIP) have a set of *Ethical Principles* and a *Code of Professional Practice* for members. CILIP's twelve *Ethical Principles* set out the principles and values on which members' conduct should be characterised and include: "*Commitment to the defence, and the advancement, of access to information, ideas and works of the imagination*" (CILIP, 2012b) whilst the *Code of Professional Practice* in relation to users, states that "*Members should therefore: Make the process of providing information, and the standards and procedures governing that process, as clear and open as possible*" (CILIP, 2012a).

We asked staff in the five case study sites whether they felt it was ethical to use filtering. Of the 31 staff we interviewed, 22 believed that it was ethical to use filtering software in public libraries while nine had some qualms. For some staff filtering was the obvious tool to implement in this environment:

> "*I don't think there is any ethical implication… We're just trying to prevent sites from being accessed that could cause offence to other people*" (ICT Manager).

Some staff spoke in terms of it being a pragmatic means to an end when providing a service to a diverse range of people:\

> "*I think inevitably when you are dealing with a whole community; you have to start thinking about if somebody was looking at a site which would be very offensive to another member of the community. I think you can't just avoid the fact… Total freedom on the Internet I think is a wonderful idea, like total freedom everywhere but if society*

> *is going to work I think there's bound to be, there has to be some restrictions*" (Library Advisor).

Staff expressing some reservation about filtering spoke in terms of it being a "*challenge*" (Assistant Director); "*unfortunate*" (Senior Manager); "*difficult*" (Team Leader); "*regret*" (Head of Libraries); "*double standard*" (Operational Manager) or a "*sensitive area*" (Desktop Services Engineer).

But some staff recognised that as a profession, filtering presented something of a dilemma to the librarian:

> "*We did think long and hard about it because in many ways filtering is anathema to librarians*" (Assistant Director).

The justification for its employment echoed that of the items reviewed for the MAIPLE project - the protection of children and young people (eight staff) and expectations of appropriateness in a public space (seven staff):

> "*What people do in their own homes is fine but in a public place there needs to be some control I think because as I say our PCs are visible to anybody here sitting out there watching something*" (Branch Library Manager).

Terms used in relation to the public nature of library space included "*insurance*" (Senior Librarian) and "*protect*" (Branch Library Manager), "*trust*" (Library Advisor) and "*safe*" (Team Leader).

The Internet users we spoke to were generally in favour of filtering; 19 users were pro-filtering and eight were unsure. Only two users did not agree that filtering software should be used by public libraries. Users in agreement with the use of filtering tended to feel that it was appropriate for a number of reasons including the presence of children in public libraries, in order for libraries to maintain standards of public decency and to ensure libraries only provide access to content which is permitted by law:

> "*I'd say so, I think in the same way you wouldn't have certain material on the bookshelves, I don't see why you wouldn't apply the same idea to internet access. I mean it's a public service and I think there are certain restrictions which you would consider decent*" (User 4).

As mentioned previously, CILIP's Code of Professional Practice states that "*Members should therefore: Make the process of providing information, and the standards and procedures governing that process, as clear and open as possible*" (CILIP, 2012a). According to the results of our survey in the majority of public library services, library users are made aware that the library employs filtering software in the AUP (88.8 per cent). Over half of responding services draw users' attention to the use of filtering software when they log-on to the PC (56.3 per cent) and over half inform the public on the library website that Internet content is filtered (51.3 per cent). Of respondents selecting 'other' (6), three services did not specifically make users aware of Internet filtering: "*We don't advertise that we use filtering software*" (Customer Service Manager). In two services, users were notified electronically either by a message on the computer screen or at the point of filtering whilst paper notifications were used in one service. In contrast, the users we spoke to in the five case study sites were almost evenly divided between those that were aware the library filtered Internet content (13) and those that were not (12). Two users did not answer. Of those that were aware, in some instances this was because they had experienced blocking (three); they had noticed it was mentioned in the service's AUP (three) or they had assumed it would be (two):

"*I'm aware that they must do something like that because there's a clause that you always agree to go on that, it more or less says that you agree to abide by their policies and procedures and I'd be very surprised in a library didn't filter the internet*" (User 3).

Of those who were not aware, some expressed genuine surprise:

> "*It is? So there are things that they just don't let you on?*" (User 2).
>
> "*I had no idea*" (User 1).

As stated previously, the most commonly used measure, after filtering software and AUPs, to manage public Internet access was visual monitoring by library staff (83.5 per cent). The staff we interviewed as part of the case studies agreed that monitoring what was being viewed on the PCs by walking around the building, for example, was a useful, if somewhat limited way, to ensure acceptable use:

> "*Where possible I'd say staff are very good just because they're out and about and sort of around their branch area. They know their customers, they know their regulars, they know somebody who's only 'they're in, they're out'. Certainly in the majority of our libraries where possible we would have adults and children separated… But I wouldn't like the responsibility to be on staff alone without proper software in place. It wouldn't work*" (Project and Service Manager).

Utilising monitoring software was also referred to as a useful tool in one case study where the majority of PCs were located in rooms not visible to staff on the front desk but there were restrictions on its use:

> "*If somebody came in and they said to somebody on the desk 'that guy over there's looking at something' or whatever then the staff do have the capability for looking at what actually is being viewed on*

> *the screen but that is only when we're given reason to do it*" (Operations Librarian).

Although another colleague in the same service expressed some concerns about its legitimacy:

> "*The system that we use here at the moment is a system called i-CAM, like a cyber café management software. It will enable the staff member to actually shadow the screen. Now as to how widely used that is, I don't think it is and the ethical implications of that are a grey area as far as I'm concerned because I don't think it actually notifies the user that they are being monitored, whereas we have software on the corporate side which does that but you need permission from the actual user for it to occur… I don't know what else we can really say about that, it's not something I would be too happy with if I was using a public machine but there we go*" (Desktop Services Engineer).

A small number of staff were dismissive of visual monitoring because they simply did not have the time to do it:

> "*We have that many other things to do nowadays it's not as if we can sit there just waiting for the next thing to… 'Oh I'll just keep an eye on that'*" (Library Advisor).

Arguably, visually monitoring use may also be ethically ambiguous as one manager proposed:

> "*I would be wholly against a member of staff walking up and down the ICT suite looking at what people are doing to be honest. It's quite draconian and an invasion of privacy because people might be doing online banking or they may be filling in forms with personal information so I'm dead against that*" (Libraries ICT Consultant).

Certainly, staff looking at what users are viewing is not a practical approach when it comes to members of the public using the library's Wi-Fi connection. At the time of the survey (2013), we found that of the 67 responding services providing Wi-Fi, the majority provided filtered Wi-Fi (83.6 per cent) while eight services provided unfiltered Wi-Fi (11.9 per cent) and three respondents did not know. This may have well changed since the online survey was carried out; in the UK there have been some significant developments in relation to public Wi-Fi. In the summer of 2013, the Department for Education and the Department for Culture, Media and Sport announced at a summit on tackling child sexual abuse online, that the main public Wi-Fi providers had pledged to offer family-friendly Wi-Fi "*in public places where children are likely to be*" (DFE/DCMS, 2013). This was to have been completed by the end of August 2013. However, media stories published in November 2013 suggested progress was patchy: "*A test of 129 free Wi-Fi hotspots around the UK including shops, cafes and children's play areas has found that 32 of them did not block access to pornhub.com, a free website that streams hardcore pornographic videos*" (Wales Online, 2013). As commercial premises providing public Wi-Fi grapple with the ramifications of access to Wi-Fi networks our results suggest public libraries in the UK were already employing filtering software. However, as our results also reveal, filtering does not guarantee that users cannot access material which may offend others. A recent media report in South West England, for example, details the account of a man charged by police after it was discovered he had been viewing pornography on the library PCs every day for more than a month (Evans, 2014). And yet, according to our survey data, this library service uses filtering software.

Conclusion

The results of the MAIPLE study suggest that public libraries' use of filtering software is a prudent solution to the problem of misuse but its presence is not easily reconcilable with a library and information professional's ethical commitment to the user's right to freedom of access to information. Our findings suggest that staff are often resigned to this approach. Suggestions for good practice arising from the project findings include:

- Decisions concerning the use of filtering software should be taken with the primary consideration of allowing the widest possible access to information for all users possible within the limits of safety and legality;
- Public libraries need to be more pro-active in alerting users to the use of filtering software and its potential impact on information access;
- Clear, simple, and well publicised policy and procedures need to be in place to enable users have sites unblocked, with respect given towards the sensitivities and privacy of users;
- Greater standardisation and harmonisation of practice would be beneficial. This could be co-ordinated through CILIP and based on guidance from the final outcomes of the MAIPLE project.

References

Australian Library and Information Association (2011). *ALIA Internet Access in Public Libraries Survey 2011*. Australia: ALIA. Available at: http://www.alia.org.au/advocacy/internet.access/Internet.Access.Survey.2011.pdf

Brophy, P. (2003). *The People's Network: A turning point for public libraries*. London: Resource. Available at: http://www.slainte.org.uk/SLIC/peoplesnet/pn_a_turning_point_2002.pdf

Byron, T. (2008). *Safer Children in a Digital World. The Report of the Byron Review*. Department for Children, Schools and Families & Department for Culture, Media and Sport, available at: http://media.education.gov.uk/assets/files/pdf/s/safer%20children%20in%20a%20digital%20world%20the%202008%20byron%20review.pdf

Cavanagh, M. (2004). Sensemaking a public library's internet policy crisis. *Library Management*, 26(6/7), pp. 351-360.

CILIP (2012a). *Code of Professional Practice*. Available at: http://www.cilip.org.uk/cilip/about/ethics/code-professional-practice

CILIP (2012b). *Ethical Principles*. Available at: http://www.cilip.org.uk/cilip/about/ethics/ethical-principles

CIPFA (2013). *Public library statistics. 2013-2014 Estimates and 2012-2013 Actuals*. London: The Chartered Institute of Public Finance and Accountancy.

Comer, A. D. (2005). Studying Indiana Public Libraries' Usage of Internet Filters. *Computers in Libraries*, 25(6), pp.10-15.

Department for Education/Department for Culture, Media and Sport (2013). *Press Release. New measures build on progress protecting childhood*. Available at: https://www.gov.uk/government/news/new-measures-build-on-progress-protecting-childhood

Evans, D. (2014). Man committed sex act while watching porn in Henbury library. *The Bristol Post*. May 06 2014. Available at: http://www.bristolpost.co.uk/Man-committed-sex-act-watching-porn-Henbury/story-21061548-detail/story.html

Hardie-Boys, N. (2004). *The People's Network: evaluation summary*. London: Big Lottery Fund. Available at: http://www.biglotteryfund.org.uk/er_eval_peoples_network_evaluation_summary_uk.pdf

IFLA (2012). *IFLA Code of Ethics for Librarians and other Information Workers (full version).* Available at: http://www.ifla.org/news/ifla-code-of-ethics-for-librarians-and-other-information-workers-full-version

IFLA (2014). *Professional Codes of Ethics for Librarians*. IFLA FAIFE. Available at: http://www.ifla.org/faife/professional-codes-of-ethics-for-librarians

LISU (2013). *Fines and Charges in Public Libraries in England and Wales 2013.* 26th edition. Compiled by Sonya White. Loughborough University.

MLA (2009). *Guidance on the management of controversial material in public libraries*. London: Museums, Libraries and Archives Council. Available at: https://docs.google.com/file/d/0B9r-dNr4kPL0aGw1dExLZTA0UnM/edit?pli=1

Pors, N. O. (2001). Misbehaviour in the public library: Internet use, filters and difficult people. *New Library World*, 102(9), pp. 309-313.

Poulter, A., Ferguson, I., McMenemy, D. & 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 2009*. Communications in Computer and Information Science (1st). New York: Springer-Verlag. Available at: http://strathprints.strath.ac.uk/29302/1/FRILLSisc02.pdf

Sommerlad, E., Child, C., Ramsden, C. & J. Kelleher (2004). *An Evaluation of the People's Network and ICT Training for Public Library Staff Programme*. London: Big Lottery Fund.

Spacey, R.E. (2003). *The Attitudes of Public Library Staff to the Internet and Evaluations of Internet Training*. Loughborough University. Available at: https://dspace.lboro.ac.uk/dspace-jspui/handle/2134/10210

Spacey, R., Cooke, L., Creaser, C. and Muir, A. (2014a). Regulating use of the internet in public libraries: a review. *Journal of Documentation.* **70**(3). Print version in press. URL: http://www.emeraldinsight.com/journals.htm?articleid=17101492&show=abstract

Spacey, R., Cooke, L., Muir, A. and Creaser, C. (2014b). Regulating internet access and content: findings from the MAIPLE project. *Journal of Librarianship and Information Science.* Print version in press. URL: http://lis.sagepub.com/content/early/2013/09/11/0961000613500688.abstract?papetoc

Sturges, P. (2002). *Public internet access in libraries and information services*, Facet Publishing, London.

UNESCO (1994). *UNESCO Public Library Manifesto*. Available at: http://www.unesco.org/webworld/libraries/manifestos/libraman.html

Wales Online (2005). Man caught downloading porn at library. *Wales Online*. 23 June 2005. Available at: http://www.walesonline.co.uk/news/wales-news/man-caught-downloading-porn-library-2393767

Ward, R. C. (2003). Internet Use Policies and the Public Library: A Case Study of a Policy Failure. *Public Library Quarterly*, 22(3), pp.5-20.