The implementation of Internet filtering in Scottish public libraries

Abstract

Purpose: This study sets out to examine the way that Scottish public library authorities are implementing filtering software as a public access Internet management tool. The aim of the study is to determine the extent to which filtering systems are used as a public access Internet management tool and to examine the nature of this implementation. This constitutes an analysis of the *actual* policies and procedures in place within each library authority to manage public access to the Internet.

Design/methodology/approach: The paper utilizes a literature review and an analysis of data supplied by the public library services. The data required was gathered through Freedom of Information requests sent to all Scottish public library authorities.

Findings: 31 of the 32 public library services operating within the 32 Scottish local authorities utilized some form of filtering software to control Internet access. The main justifications cited for this were to prevent access to illegal or inappropriate materials; however it was found that in the majority of cases the decision to implement the software was not made by the management of the library but external IT staff. This raises major issues related to the historical role of the librarian as selector of content for their community.

Research limitations/implications: The paper presents results from a subset of local authorities in the UK, thus cannot claim to be anything more than indicative of the geographic sample.

Practical implications: The findings can help inform the rationale utilized by public library services in implementing filtering policies.

Originality/value: This paper is the only paper to directly address the issue of Internet filtering in all public libraries in Scotland.

Keywords: Internet filtering; equity of access; public libraries; access policies

Introduction

The aim of the paper is to determine the extent to which filtering systems are used as a public access Internet management tool in Scottish public libraries and to examine how the tool is being utilised and managed.

Clearly access to information is a vital component of the public library mission; however the origins of the public library service also lie in a middle class Victorian proclivity to view access to education as a way of promoting the tenets of a larger moral, or perhaps 'civilising', project to the predominantly urban British underclass (Thompson, 1975). As McMenemy states, in reference to what has now evolved into the 'Great Fiction Debate', although public libraries rested firmly on the principle of equity of access it was understood that the service would constitute a place to access "high quality material and not low brow fiction" (McMenemy, 2009, p. 62). In the context of what could therefore be similarly dubbed the 'Great Internet Debate' public libraries must now wrestle with the competing desires to provide equitable access to citizens and to prevent access to materials that could be deemed inappropriate. It is then a simple and prima facie rational line of reasoning that makes reference to the 'historical project' of the public library sector, when discussing the intellectually related concepts of 'control' and 'selection'. The tendency to conflate these two separate concepts, and to miss the distinction between 'selecting to censor' and 'selecting to provide access to', is especially evident when discussing the Internet management issues connected to the installation of filtering software in a public library environment.

Writing before the advent of the Internet explosion, Hauptman summarised the tensions for the librarian in the following way:

> Much has been written concerning censorship…it is only necessary to insist that it is an ethical imperative to refuse to practice, condone, or abide any form of censorship. At the same time, censorship must never be confused with the refusal to provide socially detrimental information (in reference), the aiding and abetting of illegal acts, or the judicious selection of materials. (Hauptman, 1988, p.65)

This dichotomy lies at the heart of the Internet filtering question: on one hand providing access to the Internet is clearly a must for any library, however with this must come cognisance of the potential damage erroneous, offensive or illegal information can cause.

This paper then seeks to provide insight into how public libraries in one administrative geographic area, Scotland, are addressing the ethical and practical questions of managing public Internet access. In doing so it seeks to shed light on how such provision may acerbate and

expand historic tensions between equity of access and censorship and control that form the historical legacy of the public library service.

Literature Review

The concepts of selection, control and access were at the heart of the 'historical project' of the public library sector. This study, conducted within the Scottish public library sector, aims to examine the practical implications of these concepts with respect to public access Internet filtering software.

The People's Network

The initiatives contained within *New Library: the People's Network*, have been described as the "single largest influence on the development of ICTs in UK public libraries" (McMenemy, 2009, p.113). An initial one off grant of £100 million was provided through the National Lottery programme in order to create an ICT network in the UK public library sector. The New Opportunities Fund digitization programme (NOF-Digitize) which ran concurrently with the People's Network initiative essentially provided content that could be accessed through the ICT infrastructure and "the resulting web-portal, Enrich UK, gave access to all of the websites funded under the programme" (McMenemy, 2009, pp.119-120).

It is clear that information now has to be regarded as a concept that is platform independent and libraries have to provide multiple conduits into what has been accurately described as the "information universe" (Brophy, 2007). Although the *People's Network* has created a national ICT network infrastructure that is able to provide unfettered access to what is now a fundamental facet of this 'information universe', public libraries have sought to limit and restrict access for patrons. This is in spite of the fact that the UK's professional body explicitly states:

> "Access should not be restricted on any grounds except the law. If publicly available material has not incurred legal penalties then it should not be excluded on moral, political, religious, racial or gender grounds." (Chartered Institute of Library and Information Professionals [CILIP], 2005)

The ethical context

CILIP's *Ethical principles for library and information professionals* stresses that libraries should promote "equal opportunities and human rights" (CILIP, 2009a). Although the rights of privacy and freedom of expression enshrined in law are somewhat "limited" (Wilson and Oulton, 2000, p.195), it would be accurate to state that "a public authority providing public Internet access is acting completely within the spirit and letter of the Human Rights Act…to defend an action that someone brought against it, a public authority would have to show that what it had done in restriction of freedom of expression was the kind of exception that the law allows, and was in proportion to the problem it sought to correct" (Sturges, 2002, p.72).

Secondly CILIP stresses that libraries should show a "Commitment to the defence, and the advancement, of access to information, ideas and works of the imagination" (CILIP, 2009a). It is important to recognise here that CILIP not only advocates a passively elicited defence of the freedom to access information but urges librarians and information professionals to *actively* 'advance' this cause.

Indeed CILIP states that no item should be *a priori* prohibited from a library's collection except on the grounds that it is illegal within the jurisdiction within which the library is providing its service (CILIP, 2005). It would seem that the implementation of Internet filtering software in a public library environment would at least have some impact upon the ability of the public library sector to meet the above commitment.

Thirdly CILIP states that librarians and information professionals should show "impartiality, and avoidance of inappropriate bias, in acquiring and evaluating information and in mediating it to other information users" (CILIP, 2009a). This is an interesting and multifaceted principle. As will become clear later in the paper, by filtering information 'types' with respect to the presence or absence of keywords, there is a definite threat to the right of users to freely access information that may be 'uncomfortable' but completely legitimate and legal.

That this concern needs to be balanced with an attempt to promote the "legitimate aims and objectives of [a librarian's] employer" (CILIP, 2009b) makes this issue all the more complicated. As most library authorities are embedded within larger local government departments, or run as part of an 'arm's length' charitable trust, library managers may have difficulty communicating a

professional displeasure with certain wider departmental 'aims and objectives', of which an Internet filtering policy may be a part.

The legislative context

It is important for any library authority to remember that "any library that provides Internet access to third parties or employees, or uses a website for disseminating information, has a potential exposure to civil or criminal litigation" (Nelson, 2001, quoted in Sturges, 2002). However, although "there is certainly liability for the consequences of direct actions by members of the organisation that might result in harm to someone…there may be a possibility that this also extends to responsibility for the harm that a user of public access facilities might do either by not exercising appropriate care, or deliberately undertaking something malicious" (Sturges, 2002, p. 65). However, as Sturges then goes on to make clear, "this is likely to be dependent on the extent to which the institution has made the user's responsibilities clear to them" (Sturges, 2002, p.65).

Sturges also states that "criminal (and civil) liability for Internet content seems to lie clearly with the content provider" (Sturges, 2002, p.66). In order to make this clear Sturges remarks on the case brought against Nambla.org and the internet service provider Verio in the US District Court in Boston, "on the grounds that the site incited a man called Charles Jaynes to murder a ten-year-old boy" (Sturges, 2002, p.66). Although the website was accessed by Jaynes at the Boston Public Library no action was brought against the library authority itself.

How Internet filtering works

McMenemy and Burton identify two main approaches to Internet filtering used in public libraries: site blocking and keyword blocking. Site blocking involves "check[ing] each internet transaction against a list of banned sites. If the software recognizes a site on the banned list [of known URLs] it will not allow a computer to load up the pages from the site"(McMenemy & Burton, 2005, p.22). Keyword blocking "simply looks for offensive words in either the web address or the contents of the requested pages" (McMenemy & Burton, 2005, p.23). Again if offensive words are detected by the software then the user will be denied access to that content.

Intellectual and practical considerations

McMenemy and Burton state explicitly that "filtering of Internet content is quite simply a form of censorship. It is an acceptable form of censorship for many organisations, but it is in the raw definition of the word, censorship" (McMenemy & Burton, 2005, p. 22). Given the nature of the filtering process, its imposition within a public library context could easily be taken as a dramatic perversion of the role of the public library as an intellectually free and uninhibited provider of access to information, no matter how challenging or 'dangerous'. As Hauptman states, "it is not [a public library's] business to mediate between users and the virtual world" (Hauptman quoted in McMenemy, 2009 p. 116).

To highlight the common concerns forwarded relating to Internet filtering in a public library environment we can turn to a study conducted by Wilson and Oulton, which examines issues relating to privacy and confidentiality in public libraries across England, Wales and Scotland. There were two primary concerns raised by respondents to the study. The first related to the reliability and effectiveness of filtering software used in the public library setting, highlighting that "relevant and appropriate material was blocked" (Wilson & Oulton, 2000, p. 198). The survey acknowledged over-blocking as an inherent weakness of filtering software. Also, the large number of software packages "spontaneously cited" by respondents was interpreted as constituting a "lack of a common technical approach to filtering or blocking" (Wilson & Oulton, 2000, p. 198). This study has found no evidence to suggest that a macro-level policy decision has been made at a central level in Scotland to contradict this statement. However, it is arguable whether that approach would be desirable in itself given the idiosyncrasies within, and variations between, the different communities served by individual library authorities.

Wilson and Oulton's study highlighted the further concern that no matter how often filtering software is updated, as soon as it is updated it is out of date. Therefore, in addition to the economic costs incurred by this process there is no '*freedom from* inappropriate information' guarantee provided by the software. Further, the software, given the legitimate concern of over-blocking, has the potential to override any '*free access to* acceptable information' guarantee that any public library has the ethical duty to uphold. Resnick, Hansen & Richardson, who studied the error rates in Internet filtering software, come to the same conclusion as

Gottschalk that “education, privacy screens, honor codes, and adult monitoring” would constitute a more effective Internet regulatory system than implementing a filtering system (Resnick, Hansen & Richardson, 2004, p. 71)

These reservations were however coupled with a desire to prevent users accessing sexually explicit material through the public access terminals and it was stated that “filtering and blocking software may be considered as one way of addressing concerns that a library user may access illegal material *or* that a child may see inappropriate material in a library” (Wilson & Oulton, 2000, p. 195).

Acceptable Use Policies (AUPs)

Although Internet filtering software constitutes the focus of this study, it is thought necessary to briefly discuss the second main form of Internet management control in place within a public library environment: the AUP. A potential role for the AUP will be discussed in the conclusion section, and this section should lay the foundation for this later discussion.

The AUP is essentially a document that must be signed by a library user before they can access the Internet via the public access computers provided by the library authority. It is thus, in itself, a means of transferring liability for actions or material sought and accessed on the Internet back onto the library user rather than the library authority *directly* prohibiting access to the content. It is regularly thought of in terms of an information provider’s responsibility to younger users of the service, as it is sometimes believed that librarians and library paraprofessionals are acting *in loco parentis* and that providing protection from certain types of content is the duty of an information provider (McMenemy & Burton, 2005, p. 21).

However, there exists a position that views the AUP as an inadequate preventative tool in its own right. This understanding of the AUP views it as a clear statement of the library’s demands of its users, with Internet filtering software being understood as the ‘stick’ to make sure these responsibilities are not transgressed. This is a comfortable, and perhaps pragmatic position to advocate, however, as should be clear from the above discussion of filtering software, its ethicality is in question.

Yet issues do exist with the AUP document as a public access Internet management tool. The greatest of these issues remains the fact that if a user declines the terms and conditions of the AUP then that user will effectively be barred from a public access information service, at least partly funded by taxpayers' money. As McMenemy states:

> "The purpose of an AUP is to define what constitutes acceptable use of library facilities. This is a useful management tool for many public libraries, but at its root it challenges the principle of providing equity of access, since it defines some information as inappropriate" (McMenemy, 2009, p. 116).

The above discussion raises a further potential issue however; often this 'management tool' is not in the hands of the library professional but is regularly "linked to the existence of relevant policies at the higher local authority level" (Wilson & Oulton, p.197). There is clear potential for a serious issue to arise from this policy scenario, related to the position of the library service within the local government structure.

The public library service is likely to be part of a larger department, run by those out with the profession who may be unable or unwilling to understand the specific situation of the public library service. It may even be run by a trust or private third party which has imposed its own agenda upon the service, one which may be commercially or ideologically based. There is room here for a dichotomy to develop between the ethical guidelines dictated by the professional body (CILIP within the UK) of which the librarian may be a member, and the employer who has decided the terms and conditions of the AUP.

The AUP then is a statement detailing the responsibilities that the user has to recognise when using public access Internet facilities. However it also has the potential to detail the responsibilities of the *library* when providing free access to digital information. These could concern equity of access and free access to information that is of a legal nature, plus any *legitimate* 'in-house' rules that have to be adhered to. The AUP then has *potentially* two primary strengths: the level of control over the specific details of what constitutes acceptable access and the fact the AUP is not acting as a form of *direct* censorship.

Research gaps

The review has highlighted that several key gaps exist in the literature related to the use of Internet filtering in public libraries that need to be expanded, namely:

- What specific reasons exist that persuade public library services to adopt filtering?
- What are the categories of material blocked by the filtering?
- Which category of staff within the organisation makes the decision to adopt it?
- What mechanisms exist for the library user to challenge or have blocked materials unblocked?
- How are staff members in libraries trained regarding the issues that Internet management policies represent?

Research Aims and Methodology

The aim of the paper is to determine the extent to which filtering systems are used as a public access Internet management tool in Scottish public libraries and to examine the nature of this implementation. This will constitute an analysis of the actual policies and procedures in place within each library authority to manage public access to the Internet. To this end the research questions are:

1. How many public library authorities in Scotland include rely on Internet filtering software to manage access?
2. Where filtering software has been used as a management tool on public access terminals, what is the rationale behind this implementation?
3. If Internet filtering is implemented what types of content is the filter designed to block?
4. From what organisational level have these filtering policies been implemented?
5. Are there procedures in place whereby these policies could be overridden by staff when requested by a user?
6. What is the extent and nature of staff training procedures in place relating public access Internet filtering software?

Freedom of Information (FOI) Requests

Given that there are only 32 local authorities in Scotland, FOI requests were sent to all Scottish library authorities. The questions sent to each authority were as follows:

1) Does your Internet management policy include the use of Internet filtering software on the public access computers in your public library service?
2) What is the official rationale behind the implementation or non-implementation of filtering software on the public access computers in the public library service?
3) If Internet filtering is used in relation to the public access computers in the public library service, what type of content is the filter designed to block access to?
4) From what management level has the decision to implement/not to implement Internet filtering software on the public access computers in the public library service been taken?
5) If Internet filtering software is implemented on the public access computers in the public library service, does any member of staff have the ability to override the Internet filtering software if they deem the content blocked to be appropriate?
6) If Internet filtering software is implemented on the public access computers in the public library service, are members of staff given any training with respect to the filtering software?
7) If yes was answered with respect to the former question, what content is covered in the training?

The FOI request itself was constructed in line with the template letter to be found on the Information Commissioner for Scotland's website. It was recognised that the term 'censorship' could elicit 'inflamed' or defensive responses from authorities and therefore the request only made mention of 'Internet management tools' in general and 'filtering software' in particular.

Model FOI response and categorization of data

To give an indication of how responses were structured, the following anonymised response is included to illustrate the types of answer offered, which differed across all 31 respondents:

Table 1: Anonymised example of a library service response to the FOI query

Freedom of Information request questions.	**Library service responses.**
1. Does your Internet management policy include the use of Internet filtering software on the public access computers in your public library service?	Yes.

2. What is the official rationale behind the implementation or non-implementation of filtering software on the public access computers in the public library service?	To prevent illegal activity and to ensure that the terms of the AUP are enforced.
3. If Internet filtering is used in relation to the public access computers in the public library service, what type of content is the filter designed to block access to?	Pornography; terrorist material; content that may facilitate illegal downloading.
4. From what management level has the decision to implement/not to implement Internet filtering software on the public access computers in the public library service been taken?	Central IT services.
5. If Internet filtering software is implemented on the public access computers in the public library service, does any member of staff have the ability to override the Internet filtering software if they deem the content blocked to be appropriate?	Members of the public can request that material is unblocked but this will not be done immediately and only after careful consideration.
6. If Internet filtering software is implemented on the public access computers in the public library service, are members of staff given any training with respect to the filtering software?	There is currently no training in place which focuses on Internet filtering software.
7. If yes was answered with respect to the former question, what content is covered in the training?	N/A

Once the FOI requests had been returned, the information was then post-structured by the lead author in such a way as to ensure that the multifarious nature of the information received was represented in as accurate a manner as possible. Categories were formed with an inductive 'best-fit' or 'ground-up' rationale in mind.

The spread of answers received (illustrated in Table 1) in response to the FOI request necessitated a careful application of the above inductive approach, in order to ensure that the categories were representative of actual responses. Indeed, with respect to the following FOI question, it was initially thought best to post-structure the responses in line with the ALA's categorization of complaints against library material:

- *Cultural* (including Anti-Ethnic, Insensitivity, Racism, Sexism, Inaccurate representations)
- *Sexual* (Homosexuality, Nudity, Sex Education, Sexually Explicit, Unsuitable for a particular age group)
- *Values* (Anti-Family, Offensive Language, Political Viewpoint, Religious Viewpoint)
- *Social Issues* (Abortion, Drugs, The Occult, Satanism, Suicide, Violence) (ALA, 2009)

The rationale behind this initial approach to post-structuring was influenced by two beliefs. Firstly, that the decision to install filtering software as a public access Internet management tool in public libraries would at least partly be guided by the desire to guard against criticism of the service by members of the public. And secondly that categories set by the ALA would be grounded on experience and thus would be non-arbitrary. This approach was abandoned in favour of the careful application of inductive approach detailed above. It was thought that this would avoid any potential cultural bias and create a consistency in the method used to post-structure the FOI responses.

The inductive approach adopted arrived at the following categories for classifying the questions, based on analysis of all responses and delineating commonality of terminology/theme prevalent in responses:

Table 2: Categories adopted based on FOI questions/responses

Freedom of Information questions.	**Categories adopted**
2. What is the official rationale behind the implementation or non-implementation of filtering software on the public access computers in the public library service?	• Duty of care and reputation considerations • To prevent access to illegal and/or inappropriate content • To balance freedom of access with protection from harm • To protect vulnerable groups from inappropriate/offensive material • To protect security/integrity of council network • To ensure compliance with the AUP • Unclear from information provided • Undisclosed
3. If Internet filtering is used in relation to the public access computers in the public library service, what type of content is the filter designed to block access to?	• Sexually Explicit Content/pornography/child abuse images • Sex education • Illegal downloading (including P2P), hacking, malware and phishing

	• Weapons • Violence and extremism • Intolerance, racism and hate • Gaming websites • Gambling websites • Weapons • Drugs • Alcohol and tobacco related content • "Chat" and web-based social networking • Illegal Drugs • Web Proxies and translators • Tastless and Offensive
4. From what management level has the decision to implement/not to implement Internet filtering software on the public access computers in the public library service been taken?	• External Senior Management (non-Library) • Library Management • Joint departmental decision • Unknown • Undisclosed
5. If Internet filtering software is implemented on the public access computers in the public library service, does any member of staff have the ability to override the Internet filtering software if they deem the content blocked to be appropriate?	• Yes: Immediate Release Procedure • Yes: Non-Immediate Release Procedure • Yes: Unclear if Immediate or Non-Immediate • No Release Procedure
6. If Internet filtering software is implemented on the public access computers in the public library service, are members of staff given any training with respect to the filtering software?	• Yes: Specific to filtering software • Yes: Specific to filtering software but only to nominated staff members • Yes: General training covers filtering software • No Training • Undisclosed
8. If yes was answered with respect to the former question, what content is covered in the training?	• Referral procedure for blocking/unblocking web content • General overview and basic use of the software • Basic filtering terminology • Relationship between filtering and the AUP • Internet safety and child protection online

All of the thirty two Scottish unitary authorities contacted as part of the Freedom of Information responded within the 20 working day period as stipulated within the Freedom of Information (Scotland) Act 2002 (FOISA). 31 of the 32 provided the information requested, with one

authority refusing to provide the information requested, within the terms of the freedom of information request.

Results and Analysis

Results of the FOI responses are displayed below under each research question.

Research question 1: How many public library authorities in Scotland include rely on Internet filtering software to manage access?

The FOI request revealed that 31 of the public library services operating within the 32 local authorities across Scotland utilise some form of Internet filtering software as a method for controlling public access to the Internet.

Research question 2: Where filtering software has been used as a management tool on public access terminals, what is the rationale behind this implementation?

Figure 1 begins to reveal the official reasons why 31 Scottish local authorities have chosen to use filtering software as an Internet management tool on their public access computers.

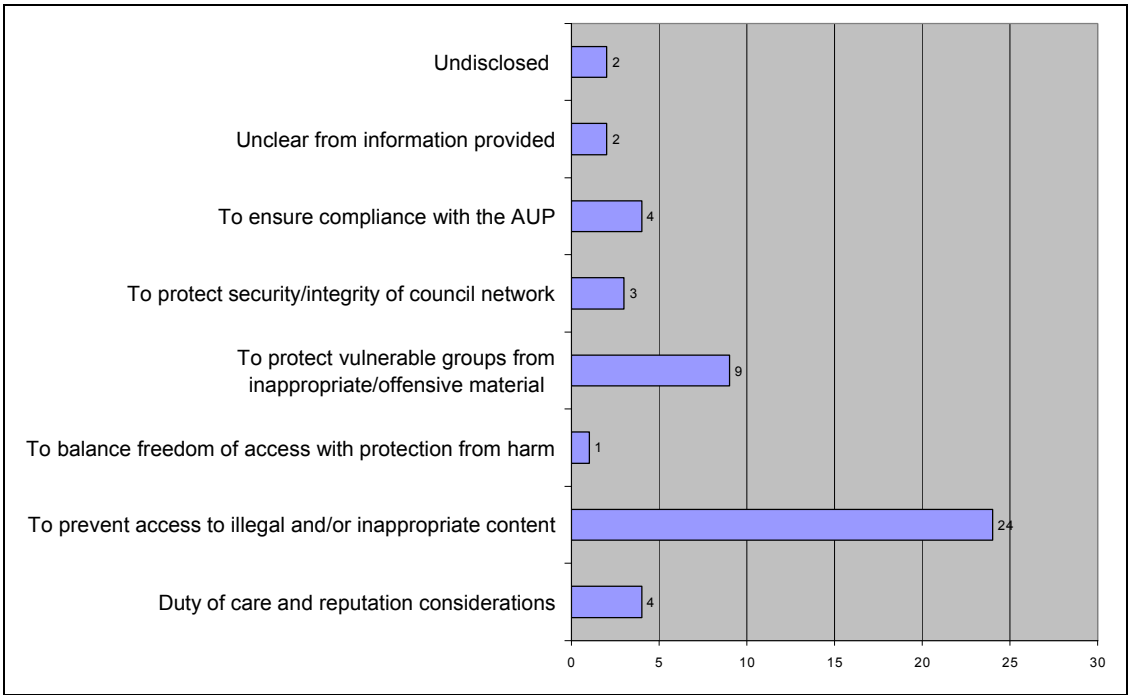

Figure 1: Official rationale behind the implementation of Internet filtering software in Scottish public libraries (more than one option could be selected) (max n=31)

The Figure offers instances of individual reasons given for why Internet filtering software was installed, although each service provided a multi-faceted rationale lying behind their decision. Given the broad nature of this short study, it was thought that the general overview afforded by the analysis in Figure 1 would suffice. A more nuanced examination focused on each multi-faceted rationale could form the basis of a further study.

The analysis above provides the following data: 24 local authorities cited 'preventing access to illegal and/or inappropriate content' as a reason for using Internet filtering software as a public access management tool. This was by far the most common reason afforded by the Scottish public library services.

The second most common reason, cited by 9 local authorities, stated that the filter was at least partly designed 'to protect children and vulnerable users from inappropriate material.' The term

'vulnerable user' was considered to constitute adults defined as vulnerable within the terms set out in the Adult Support and Protection (Scotland) Act 2007.

4 local authorities considered the public access Internet filter a means of 'ensuring compliance with the AUP' and the same number again implemented a filtering system in line with 'duty of care and reputation considerations.' 3 local authorities stated that the public access Internet filter was in place to 'protect the security or integrity of the council computer network' and 1 authority stated that is was implemented as a means of balancing the competing concerns of free access to information with a right to protection from harm.

In 2 instances it was unclear from the information provided what the official rationale behind the implementation of public access internet filtering software may have been (this has been labelled 'unclear from information provided'). A further 2 library authorities withheld this information (these responses have been labelled as 'undisclosed').

Research question 3: If Internet filtering is implemented what types of content is the filter designed to block?

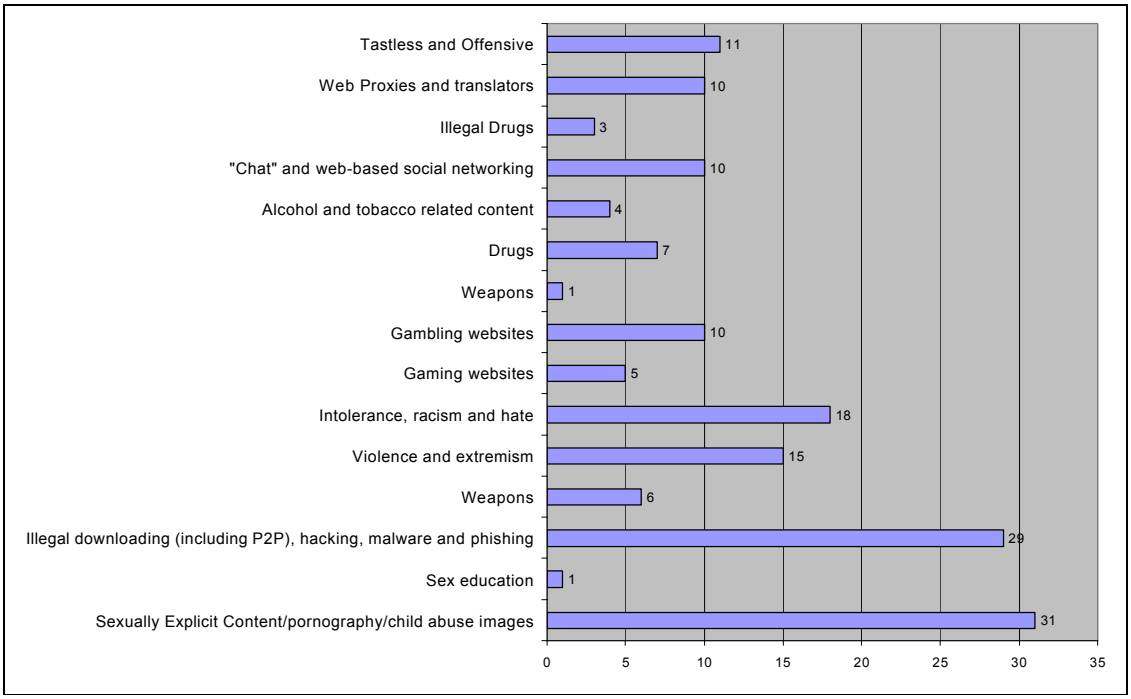

Figure 2: Type of content Internet filtering software is designed to block in Scottish public libraries. (more than one option could be selected) (max n=31)

Figure 2 represents the type of content filtered by each service, and the responses begin to reveal a broadly tripartite split in the type of content being filtered along the following lines: *'actual illegal content/activity'* (sexually explicit content/pornography/child abuse images; online illegal downloading, hacking, malware and phishing; illegal drugs); *'potentially illegal content/activity'* (web proxies and translators; drugs; weapons; intolerance, racism and hate; violence and extremism; weapons) and *'value judgement grounded'* (tasteless and offensive; chat and web-based social networking; alcohol and tobacco related content; gambling websites; gaming websites; sex education).

Any of the above given content types is of course not necessarily fixed to one single category (for example 'illegal drugs' could come under both actual and potentially illegal content', given the nature of the topic itself, or a value judgement, if the decision to block the content was based on an intention to filter out even legal and 'appropriate' discussion surrounding the topic) within this tripartite split, and as an explanatory tool it is by no means a perfect fit for the data.

However, it does help to reveal trends in the data and it provides a more than adequate platform from which the discussion of filtered content will follow.

Research question 4: From what organisational level have these filtering policies been implemented?

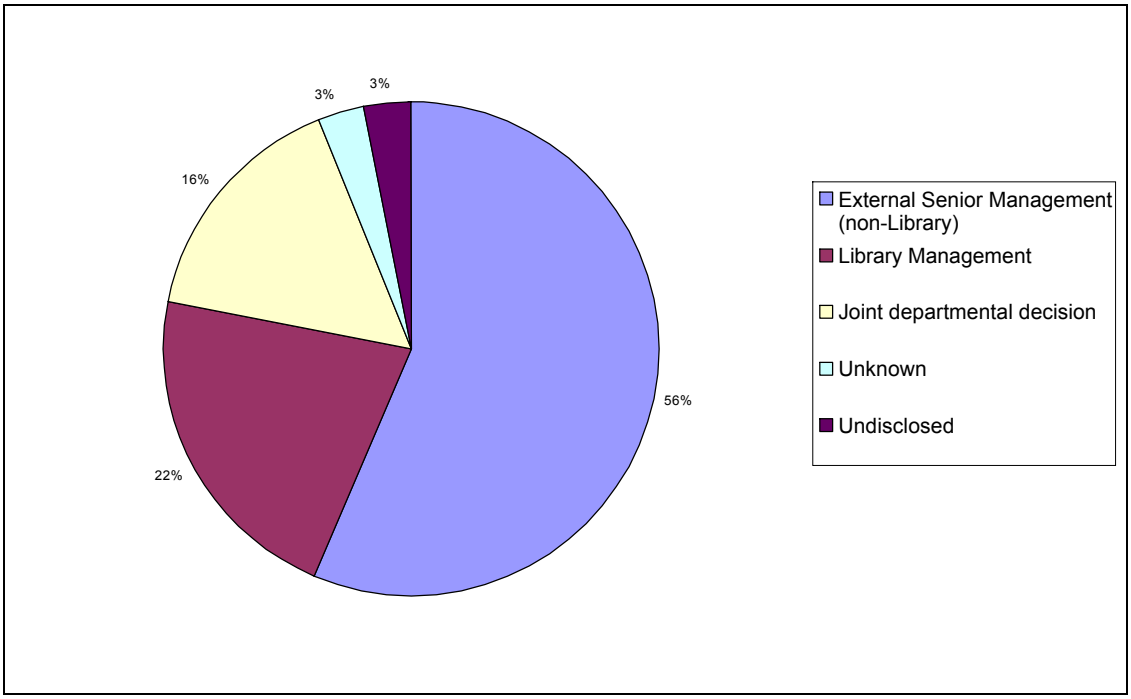

Figure 3: Source of policy decision to implement/not to implement Internet filtering on public access computers (n=32).

Figure 3 details the source of the policy decision to implement or not to implement Internet filtering on public access computers. The results were as following: 18 (56%) local authorities stated that the decision was made by external senior management, out with the service itself; 7 (22%) local authorities stated that the decision was made by a management team within the library service; 5 (16%) local authorities stated that the decision constituted a joint departmental decision between library service management and a management team out with the service, and 1 (3%) local authority stated that they were unaware of the source of the policy decision to implement Internet filtering on the public access computers (this response has again

been labeled ‘unknown’). 1 (3%) local authority declined to respond to this question (this response has been labeled ‘undisclosed’).

Research question 5: Are there procedures in place whereby these policies could be overridden by staff when requested by a user?

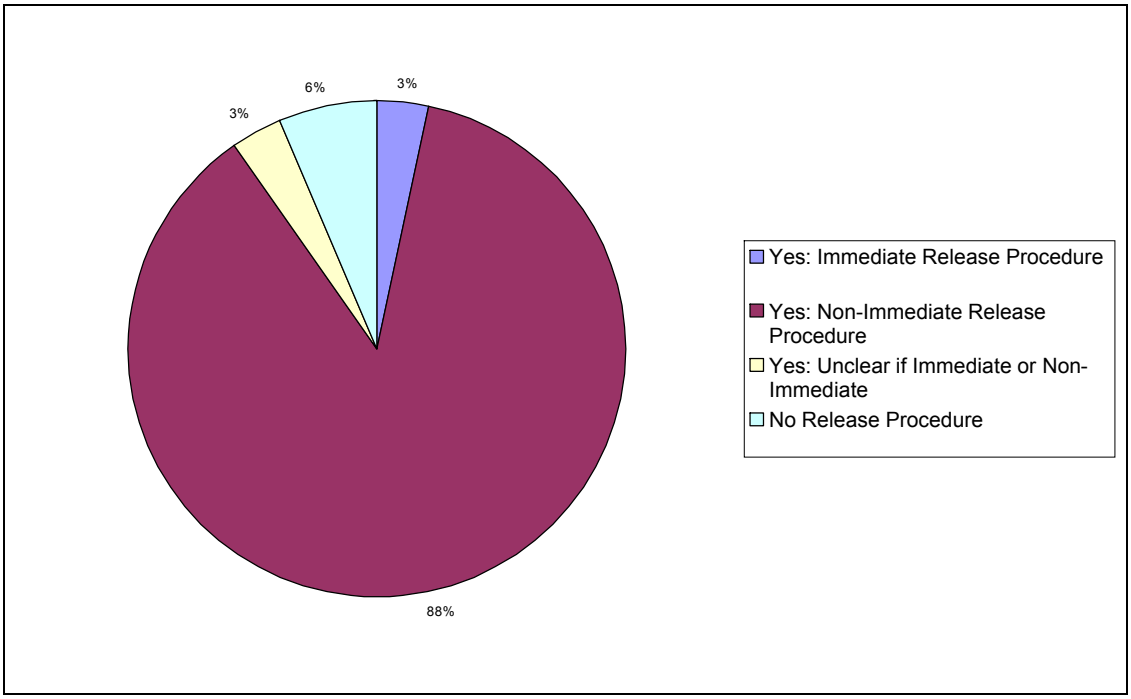

Figure 4: Procedure to release information blocked by the Internet filtering software (n=31).

Figure 4 details whether or not there exists a procedure whereby content blocked by the filter that is, on inspection, deemed “appropriate” by the service, can then be unblocked. The results were as follows: 1 (3%) local authority stated that frontline staff had the ability to immediately release content blocked by the filter, if deemed appropriate, at the point of use (‘immediate release procedure’); 27 (88%) local authorities stated that although there was a ‘release procedure’ in place, the content could not be released at point of use. It would rather be considered ‘appropriate’ retroactively and released at a later date (‘non-immediate release procedure’); 2 (6%) local authorities stated that no procedure existed whereby content blocked

by the public access internet filtering software could be released ('no release procedure'). 1 (3%) local authority responded by stating that a release procedure was in place, however it was unclear from the response whether this procedure was immediate or non-immediate and has been labelled accordingly in Figure 4.

Research question 6: What is the extent and nature of staff training procedures in place relating public access Internet filtering software?

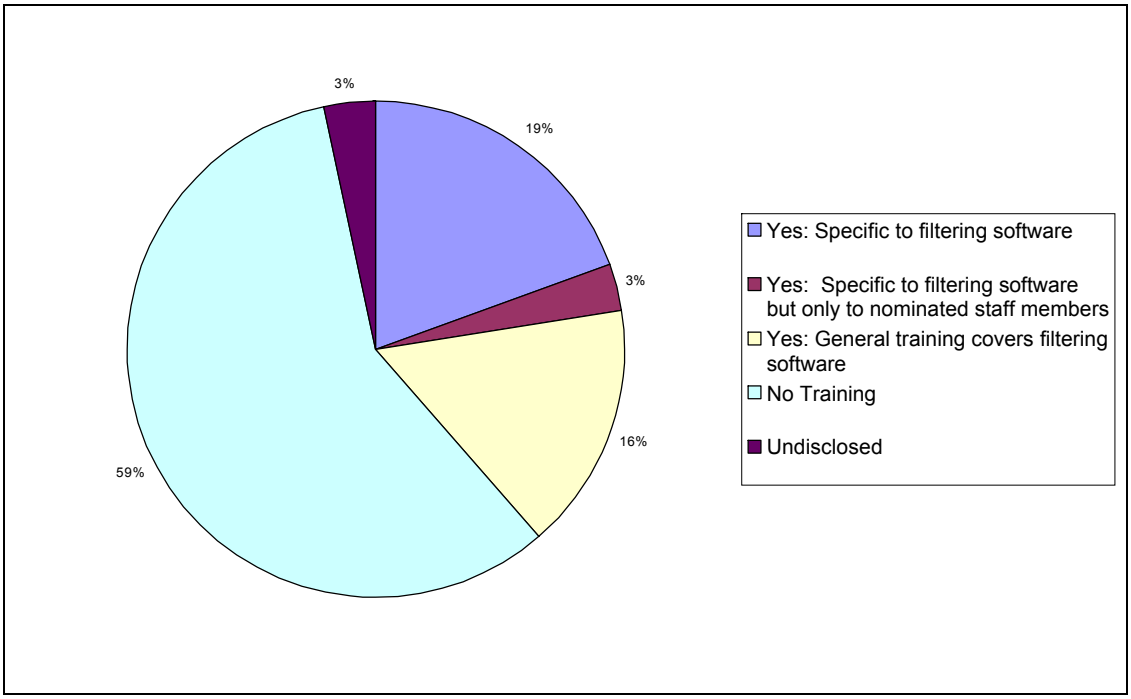

Figure 5: Staff training relating to Internet filtering software (n=31).

Figure 5 shows the prevalence of staff training, relating specifically to issues connected to Internet filtering, in Scottish public libraries. 18 (59%) local authorities stated that they did not offer any training to staff within the library service that concentrated on issues relating to Internet filtering; 6 (19%) local authorities stated that they offered library staff specific training on issues relating to public access internet filtering software; 1 (3%) local authority stated that although they offered specific training covering issues relating to public access internet filtering software this was only administered to nominated staff members; 5 (16%) local authorities

stated that their general staff training covered issues relating to public access internet filtering software but that there was no specific training offered. 1 (3%) local authority declined to respond to this question (this response has been labeled 'undisclosed').

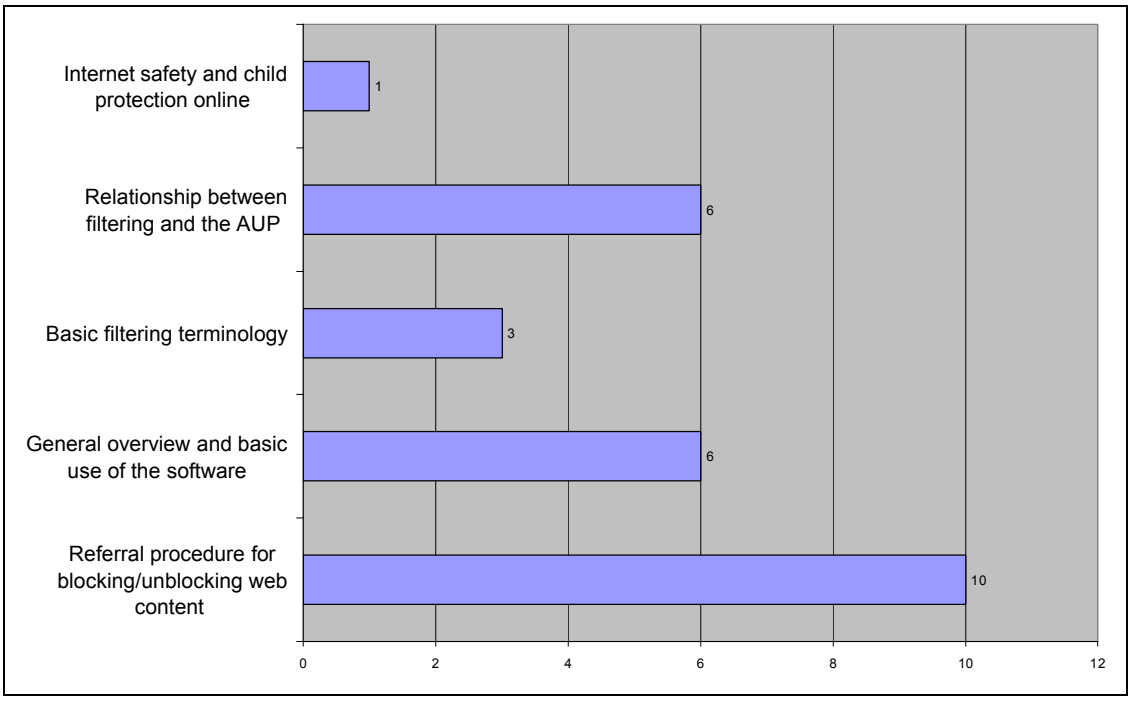

Figure 6: Content covered by Internet filtering software training (max n=12).

Figure 6 provides an analysis of the content covered by the 12 local authorities that stated that they did offer some form of training that covered issues connected to public access Internet filtering. The analytic breakdown was as following: 10 local authorities stated that their staff training covered the 'referral procedure for blocking/unblocking web content'; 6 local authorities stated that their training constituted a general overview of the software and its basic use; 6 local authorities stated that the relationship between Internet filtering and the AUP was covered within the training offered; 3 local authorities stated that their training covered 'basic filtering terminology' and 1 local authority stated that their staff training covered issues related to 'internet safety and child protection online'.

Discussion of results

The rationale, policy decision making procedures and purpose of public access Internet filtering

The FOI request results highlighted that 31 of the 32 public library services operating within the 32 Scottish local authorities utilise some form of filtering software as a method for controlling public access to the Internet. This discussion section will examine the results.

As was stated earlier, Sturges emphasises that "a public authority providing public internet access is acting completely within the spirit and letter of the Human Rights Act" (Sturges, 2002, p.72). Again, as was stated above, a public library authority could restrict access to Internet content on the basis of it constituting a 'protection of morals'. Indeed the FOI request seems to have highlighted that the decision to block certain category types *appears* to be grounded upon value judgements (whether they constitute moral judgements or not is a moot point) rather than the specific illegality of the potential material that could be accessed if the category type was left unfiltered.

As was stated above, there appears to be a broadly tripartite split in the type of content public access internet filtering is designed to block: *'actual illegal content/activity'* (sexually explicit content/pornography/child abuse images; online illegal downloading, hacking, malware and phishing; illegal drugs); *'potentially illegal content/activity'* (web proxies and translators; drugs; weapons; intolerance, racism and hate; violence and extremism; weapons) and content blocked on the grounds of the basis of an apparent value judgement i.e. *'value judgement grounded'* (tasteless and offensive; chat and web-based social networking; alcohol and tobacco related content; gambling websites; gaming websites; sex education).

Given the spread of these categories there is real potential to conflate 'objectionable material' with illegal material. As Sturges states, "when people describe internet content as harmful they tend to lump together both legal and illegal material" (Sturges, 2002, p.21). This potential issue is not restricted to the material that is ostensibly being blocked on the basis of a value judgement.

Although it may be possible to rationally defend restricting access to *legal* pornographic material on public access computers in a public library, it is less clear that placing a blanket restriction on accessing *information on* 'illegal drugs', 'violence', 'racist material' and 'weapons' is prima facie justifiable given that this could stifle legitimate (and legal) research. In instances such as this, it may be preferable to create an age appropriate 'walled garden' of accessible sites that provide information on topics such as illegal drugs.

Yet of course the public library service, perhaps concerned with its own civil responsibilities or even the potential for civil actions to be taken against it, must also consider users of the wider service who may view material accessed, via the public access Internet computers, by another user. This is perhaps tacitly reflected in many of reasons local authorities cite for installing Internet filtering software: to prevent access to illegal and/or inappropriate content; to protect vulnerable groups from inappropriate/offensive material; to meet duty of care and reputation concerns and to balance freedom of access with protection from harm

Further to this, 4 library authorities viewed the Internet filtering software as a means of ensuring adherence to the terms of the AUP, which is itself a means of passing responsibility for access onto the user and freeing the library authority from liability for any offense that may be caused as a result of users accessing 'inappropriate' material. This would seem to constitute a sound legal judgement, especially in light of what was said with respect to the 2010 Digital Economy Act (indeed 29 library authorities already state that their filter was designed to block access to sites that would facilitate 'illegal downloading, hacking, malware and phishing), and Sturges states that "providing unfiltered or insufficiently supervised access might well be taken as taking insufficient care to prevent something like this happening" (Sturges, 2002, p.77). Although this study holds that a robust AUP combined with Internet monitoring and an educative campaign within public libraries *should* constitute reasonable care, such examples highlight the difficulty a library professional has in balancing ethical commitments to access with legal precautions and considerations.

However, simply considering certain information as 'harmful' or 'inappropriate' and implementing measures that will prevent users from accessing such information on that basis alone is a dubious stance to take. Although a librarian, as a professional, *may wish* to take a

personal moral stance with respect to certain material this study suggests that library and information professionals should attempt to operate with the ethical framework provided by CILIP: that access to information should be blocked on legal grounds alone. And, as appears from the literature to be a stance more commonly adopted by the ALA, if the implications of certain acts of legislation appear to erode civil liberties to unjustifiable extent, then action should be taken against that legislation.

There is of course a possible source of tension here. As the results section highlighted, in 18 instances the decision to implement Internet filtering on public access terminals was taken by management out with the library service. In 5 cases this was a joint decision taken between local authority departments and in only 7 cases was the decision taken by the library authority's management team. There is real evidence that in the Scottish context, the decision making processes underlying the implementation of public access Internet filtering often lie out with the sector, which has the potential to impact upon a librarian's sense of responsibility for this software.

This study recognises that library authorities form only one service within the larger local government structure within which they are embedded. It also recognises that the "legitimate aims and objectives of [the] employer", a point incorporated into CILIP's *Code of Professional Practice*, need to be considered when public services are being delivered to users. However this study also advocates that if public access Internet filtering is in place then the relevant library management team must have some measure of control over the content being either initially or retroactively filtered, even if they were not part of the initial team who decided to implement the filtering software. Further issues relating to professional practice are discussed below in the sections covering staff training and censorship and the effectiveness of filtering software. Finally, in two instances, it was unclear from the information provided by the local authorities as to what the rationale was behind the implementation of public access internet filtering. In one further case the local authority was unable to state from what management level the decision implement this filtering software was taken. In the first two cases it is unclear whether or not this uncertainty is procedural or simply an unclear response.

However, in the latter case, given what has already been stated concerning the nature of public access Internet filtering and its potential to act as a form of censorship, it is important that every aspect of the decision process undertaken when implementing public access internet filtering software is accounted for and understood. It should therefore be unacceptable that any local authority or body running a public library service is unaware of the policy source responsible for implementing filtering software as a public access Internet management tool.

Procedures in place to release 'appropriate' information

Given what has been stated above concerning the position of the public library service within a larger local government structure, it perhaps unsurprising that only one local authority operates an 'immediate' release procedure exists in Scottish public libraries. Communication should be placed at the heart of this aspect of service delivery and this study does not advocate the implementation of immediate release procedures as a necessity. Indeed if an 'immediate' procedure was implemented, then the potential for the "legitimate aims and objectives of [the] employer" to be overlooked may become more realistic as individual staff members override the filter without further consultation.

However this study does make two recommendations in this area. Firstly, that any library authority does not have in place a procedure to override the public access Internet filter is unacceptable. This situation could easily stifle completely legitimate research and passively allows the filter to become an instrument of censorship. The first recommendation in this area then advocates that the relevant library authorities implement, in conjunction with their local authority, an Internet override procedure and that the ethical guidelines of CILIP (stating that material should not be restricted except on the grounds that it is illegal) guide its implementation and use.

The second recommendation provides a link to the issues connected to staff training and is based on the fact that only 10 library authorities stated that they offered staff training that focused on the procedure required to be followed to in order to unblock legitimate content. Although this constitutes a high proportion of the authorities that offer staff any form of staff training (83%) in this area, it remains low with respect to overall number of authorities that

implement public access internet filtering (32%). This study recommends that content covering this issue is developed and integrated into present staff training structures.

Internet filtering software and staff training

The way in which information is being sought out and consumed, as well as the way we communicate with each other, is changing and the locus of this change is technology. These new technologies generally fall under the rubric of what has been given the term 'Web 2.0'. O'Reilly offers us the 'compact definition' of Web 2.0 as "the network as platform…Web 2.0 applications are those that make the most of the intrinsic advantages of that platform; delivering software as a continually updated service that gets better the more people use it" (O'Reilly, 2005).

Public libraries appear to be adopting these technologies as an important method of delivering their services (Secker and Price, 2008, pp.62-65). However, the adoption of these technologies must be part of a larger strategy for delivering digital content to the user. This can be achieved by bringing the digital library model within the traditional library framework. Although the concept of a digital library is by no means fixed in the literature, it is being used here in the following sense: a public library service selecting and providing access to information and material in digital form, whether this information is 'born digital' (i.e. originally created in a digital format) or a digitised copy of a tactile original.

Staff competence in ICT was to be achieved through each local authority applying for their share of the £20 million allocated by the NOF for staff training purposes (Library and Information Commission, 1998). However, it is recognised that in order to maintain the level of understanding that would allow all members of staff to act as effective intermediaries between the user and digital content, a consistent reappraisal of the computer literacy of public library staff is necessary.

It has been reported that negative perceptions were held by public library staff towards both ICT and ICT training (Jones et al. 1999). As ICT and Web 2.0 technologies become central to the way in which society accesses and consumes information it is imperative that public library staff are able to perceive two aspects of what Davis calls the 'Technology Acceptance Model', that is both the 'ease of use' and the 'usefulness' of the technologies themselves (Davis, 1989). This should

also allow traditional hierarchies to function properly and the "pecking order" to remain in place as those higher up in the service, holding professional library qualifications, do not have to rely, to an unnecessary extent, on paraprofessionals below them due to their own ICT incompetence (Spacey, Goulding and Murray, 2003, p. 65).

However, this study has highlighted a potential discrepancy between the usefulness and necessity of staff training that focuses on the issues connected to the implementation of filtering software on public access Internet computers and its provision within the Scottish public library sector. 18 library authorities stated that they did not offer any training that either generally or specifically concentrated on issues relating to Internet filtering, and only 6 authorities offer specific training in this area to all members of staff.

This study contests that *effective* staff training should, at a minimum, approach the issues connected with public access Internet filtering. This training schedule, coupled with annual employee development conferences to analyse the strengths, weaknesses and needs of staff, should help Scottish public library services achieve an acceptable level of staff competence in ICT and maintain the sector's position at the heart of information provision in a world of fast paced technological development. As a point of good professional practice this should be carried out whether library staff are directly or indirectly responsible for administering public access internet filtering software.

Conclusions and recommendations

This study has examined the following areas related to the use of filtering software as an Internet management tool:

- The rationale and purpose of public access Internet filtering grounding the use of filtering software as an Internet management tool in Scottish public libraries.
- The policy source responsible for installing filtering systems on public access Internet computers.
- The procedures in place to manage public access Internet filters in Scottish public libraries.

- The extent and nature of staff training procedures in place relating to public access Internet filtering software.

Gottschalk argues that Internet filtering is not an appropriate solution or response to concerns relating to access of inappropriate material in a public library context. She proposes a tripartite approach grounded upon "the use of computer equipment with privacy screens or recessed monitors and the establishment of an Internet use policy in combination with the education of library users to maintaining the libraries' role as valued centers for free self-education and learning" (Gottschalk, 2006).

However, this study recognises the practical reasons grounding the implementation of filtering software as a public access Internet management tool and recognises that its use may sadly have become a pragmatic necessity. As such this study makes two primary recommendations: that a more systematic programme of training, which addresses the issues connected to Internet filtering software, is further developed and integrated into the present staff training structure within the various library services across Scotland. And secondly that there is further discussion at a national level which analyses the role Internet filtering software is playing within library services throughout Scotland.

The issue of 'inappropriate public use' could be defined in line with the ethical guidance provided by the relevant professional body and any acts of legislation that apply to the jurisdiction within which the public library authority delivers it service. Used in conjunction with an AUP this would arguably constitute a more suitable response to Internet management in a public library setting than would a policy of using software to filter out inappropriate 'types' of content.

Implementing a firm AUP passes liability back onto the user and provides the librarian with an opportunity to avoid practices that constitute the direct censoring of information. Although issues concerning access remain (if a user refused to sign the agreement then access would be denied) it would be difficult for a user to legitimately argue against an AUP that restricts access on legal grounds alone, unless an argument was being made against the legal grounds themselves.

However, as Sturges states, public access Internet facilities should complement those used for private access. They are not simply a means of "preventing social exclusion" but rather offer "the extra potential of access that is supported by professional guidance" (Sturges, 2002, p.11). Although stressing within an AUP that your authority cannot be held liable for the action of any given user may be legally sound, and in this litigious age most probably necessary, as an information provider it is not enough to pass on the legal buck and then rest easy.

Limitations and recommendations for further research

This study cannot claim to be definitive; however given its coverage of the Internet management policies in place in an entire administrative geographic region, it is believed its findings offer good insight into how such policies are adopted. Nevertheless the authors acknowledge that the data gathering mechanism, Freedom of Information queries, are limited in terms of reliance on the answers provided by each library service. The inductive approach to categorisation adopted as a result of the differences in these responses results in an element of subjectivity related to the terminology utilised in the categorisation.

However the authors believe that serious issues have been raised as a result of the research conducted for this paper. The public library is an important institution in society; however it must seek to balance access to information with appropriate duty of care to society in ensuring that citizens are protected from inappropriate materials.

Further research is recommended examining:

- The extent the finding in this study related to the majority of library services having their Internet filtering policy specified by staff out with the library service is replicated in other regions
- The consistency of categories of material blocked across other geographic regions
- The policies in place related to unblocking sites blocked in error by the filtering software
- The impact on users of blocking of material of a sensitive nature
- The feasibility of a one size fits all model for the development of a universal public library Internet management policy.

References

Auld, H.S. (2005). 'Do Internet filters infringe upon access to material in libraries?' *Public Libraries*, 44 (4), pp. 196-204.

Brophy, P. (2007). *The library in the twenty-first century* (2nd ed.). London: Facet.

CILIP (2005). *CILIP Statement on Intellectual Freedom, Access to Information and Censorship*. London: CILIP.

CILIP (2009a). *Ethical principles for library and information professionals*. Available at: http://www.cilip.org.uk/get-involved/policy/ethics/pages/principles.aspx [last accessed 19/03/2011].

CILIP (2009b). *Code of Professional Practice*. Available at: http://www.cilip.org.uk/get-involved/policy/ethics/pages/code.aspx [last accessed 19/03/2011].

Davis, F.D. (1989). 'Perceived usefulness, perceived ease of use, and user acceptance of information technology.' *MIS Quarterly*. 13, 319-39.

Gottschalk, L. (2006). *Internet Filters in Public Libraries: do they belong? Library Student Journal*. Available at: http://www.librarystudentjournal.org/index.php/lsj/article/view/25/17 [last accessed 20/9/2011].

Hauptman, R. (1988) *Ethical Challenges in Librarianship*. New York: Oryx Press.

Jones, B. Sprague, M. Nankivell, C. Richter, K. (1999). *Staff in the New Library: Skill Needs and Learning Choices. Findings from Training the Future, a Public Library Research Project*. British Library Research and Innovation Report 152. London: British Library.

Library and Information Commission (1998). *Building the New Library Network*.

McMenemy, D. & Burton, P. (2005). 'Managing access: legal and policy issues of ICT use' in

McMenemy, D. & Poulter, A. (eds.) *Delivering Digital Services: A handbook for public libraries and learning centres*. London: Facet.

McMenemy, D. (2008). 'Internet access in UK public libraries: notes and queries from a small scale study.' *Library Review*, 57 (7), pp. 485-489.

McMenemy, D. (2009). *The Public Library*. London: Facet.

O'Reilly, T. (2005a). Web 2.0: a compact definition? *O'Reilly Radar Blog*. Available at: http://radar.oreilly.com/archives/2005/10/web-20-compact-definition.html [last accessed 3/8/2011]

Resnick, P. Hansen, D.L & Richardson, C.R (2004). 'Calculating error rates for filtering software.' *Communications of the ACM*, 47 (9), pp. 67-71.

Secker, J. and Price, G. (2008). Libraries as a Social Space: enhancing the experience of distance learners using social software. In: Brophy, P. Craven, J. and Markland, M. (eds.) *Libraries Without Walls 7: Exploring 'anywhere, anytime' delivery of library services: Proceedings of an international conference held on 14-18 September 2007, organized by the Centre for Research and Information Management (CERLIM), Manchester Metropolitan University*. London: Facet.

Sobel, D.L. (2003). 'Internet Filters and Public Libraries.' *First Amendment Center*, 4 (2).

Spacey, R. Goulding, A. and Murray, I.R., 'ICT and Change in UK Public Libraries: Does Training Matter?' *Library Management*, 24(1/2), 2003, pp 61-69.

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

Wilson, J. & Oulton, T. (2000). 'Controlling access to the Internet in UK public libraries'. *OCLC Systems & Services*, 16 (4) : 94-201.