Regulating Internet access and content in UK public libraries: findings from the MAIPLE project

This item was submitted to Loughborough University's Institutional Repository by the/an author.

Citation: SPACEY, R.E. ... et al, 2015. Regulating Internet access and content in UK public libraries: findings from the MAIPLE project. Journal of Librarianship and Information Science, 47 (1), pp. 71-84.

Additional Information:

- This article is distributed under the terms of the Creative Commons Attribution 3.0 License (http://www.creativecommons.org/licenses/by/3.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed.

Metadata Record: https://dspace.lboro.ac.uk/2134/14436

Version: Published

Publisher: Sage (© the authors)

Rights: This work is made available according to the conditions of the Creative Commons Attribution 3.0 Unported (CC BY 3.0) licence. Full details of this licence are available at: http://creativecommons.org/licenses/by/3.0/

Please cite the published version.
Regulating Internet access and content in UK public libraries: Findings from the MAIPLE project

Rachel Spacey
Loughborough University, UK

Louise Cooke
Loughborough University, UK

Claire Creaser
Loughborough University, UK

Adrienne Muir
Loughborough University, UK

Abstract
This paper reports the results of an online survey concerning the management of Internet access in UK public libraries. All UK public library authorities were invited to complete the survey which had a response rate of 39%. The survey explored the ways in which acceptable use of the Internet in public libraries is managed through the use of mechanisms such as filtering software and authentication of identity. All 80 responding public library authorities used filtering software. Procedures for authenticating identity for static Internet access were uniform whereas wireless access was much less regulated.

Keywords
Copyright, filtering, Internet, misuse, public libraries, Wi-Fi

Introduction
This article presents the preliminary quantitative results concerning the management of Internet access in UK public libraries collected as part of the Arts and Humanities Research Council (AHRC) funded MAIPLE (Managing Access to the Internet in Public Libraries) project. One of the key purposes of the public library is to provide access to information (UNESCO, 1994). In the UK, Arts Council England, the non-departmental public body of the Department for Culture, Media and Sport (DCMS) which has responsibility for supporting and developing libraries recently noted that public libraries: ‘build a healthy democracy by providing free access to reliable information through which we form our opinions’ (Arts Council England, 2013: 4). Information is available in public libraries both in printed formats and via the provision of public access Internet workstations. However, to date there has been little research undertaken to investigate how UK public libraries manage issues of misuse and content control of their public Internet provision, including the access of illegal material. In the UK such material includes sites with images of child sexual abuse or which incite racial or religious hatred and/or violence. Indeed, it has even been suggested that, despite the information profession’s espousal of a commitment ‘to provide, as far as resources allow, access to all publicly available information’ (CILIP, 2005),

Corresponding author:
Rachel Spacey, LISU, Centre for Information Management, Loughborough University, Loughborough, LE11 3TU, UK.
Email: r.e.spacey@lboro.ac.uk
in the UK such is the low level of attention paid to this issue, that ‘filtering software in public libraries seems, in practice, to have “crept in through the back door” with little more than a murmur on the part of librarians’ (Cooke, 2006). The aim of the MAIPLE project, therefore, is to address this lack of factual awareness, providing a comprehensive picture through identifying and quantifying measures currently in place across the UK to regulate access to Internet content in public libraries.

The article begins by providing a brief overview of some of the key UK literature on the topic (a more in-depth discussion of this literature, together with international examples, can be found in Spacey et al., 2013). It then describes the methods used by the research team, before presenting some of the key quantitative findings to date. The paper concludes by highlighting some of the more important themes emerging from the findings and discusses their implications for practitioners and policy makers.

**Literature review**

**Managing access to the Internet in public libraries: Research from the UK**

During 2011 to 2012, public libraries in the UK provided the public with Internet access through 43,365 terminals offering a potential 83,436 hours and actual 35,819 recorded hours of usage over 4384 service points (CIPFA, 2012). This infrastructure means that adults and children may participate in the digital sphere in an environment in which trained staff are able to support them and help them develop their digital skills. As recent research carried out for the Carnegie UK Trust argued:

Public libraries have been involved in enabling digital participation among those at risk of exclusion from on-line services, such as older people. There is evidence from England that half of those who do not have access to the internet at home, but use the internet in public places, do so in a public library. Libraries have a clear role in supporting life-long learning through their involvement in IT support for library users. (MacDonald, 2012: 20)

Public libraries are steered in their provision of Internet access by a desire to provide equity of access to this technology, both prior to and subsequent to the introduction of the People’s Network (PN), a national network of PCs in public libraries providing Internet access whilst being mindful of their legal obligations in relation to copyright and privacy.

Much of the research relating to public library Internet access in the UK dates from the development of the PN when funding of £100m was dedicated, in the late 1990s, to provide the infrastructure to connect all static library points to the Internet and £20m was assigned to train all public library staff in the UK (see, for example, Brophy, 2003; Sommerlad et al., 2004). Some recent research has looked at mapping wireless Internet access (Wi-Fi) availability in public libraries (Batt, 2009) and in relation to the management of public Internet access in Scottish public libraries (Brown and McMenemy, 2012).

One of the earliest papers charting Internet access in public libraries was by Willson and Oulton (2000) who reported the results of a project which looked at privacy, anonymity and confidentiality in public libraries. Responses were received from 111 Public Library Authorities (PLAs) in England, Scotland and Wales. The survey explored Internet access, policy and controls including software. PLAs were questioned about controls such as the use of blocking and filtering software on both public access and staff only PCs. The most common filtering technique is that of content analysis or ‘the controlling of information based on the analysis of specific keywords within web pages or URLs’, whilst blocking relies on denying access to specific Internet Protocol addresses (Hamilton, 2004: 156). More PLAs imposed controls on public access PCs than did so on staff only PCs (71% compared with 56%), which might include visual monitoring such as having PCs in public areas observable by staff and the public. Filtering was the most popular control on public access PCs (52%) followed by blocking controls (23%) and monitoring (16%). Issues emerging from the use of controls included over-blocking and users unable to access legitimate sites. Those in favour of controls were usually concerned with sexually explicit and/or racist material being accessed. Those against the use of controls were more accepting of their use on the PCs in the children’s library but preferred PCs in public areas to be visible and to become self-regulating. Policies relating to electronic content were more directly and publicly accessible in the form of Acceptable Use Policy (AUP) posters near Internet terminals compared to policies relating to print materials which were often included in mission statements or stock selection policies. Indeed, Willson and Oulton (2000) highlighted the two key mechanisms by which public libraries have continued to manage Internet access in public libraries: AUPs and content control.

**Acceptable use policies.** McMenemy and Burton (2005) in a book aimed at public library professionals in the UK, dedicated a chapter to the management of ICT access. They considered the two main methods used in public libraries: AUPs and filtering. AUPs are usually documents which detail activities which are not permitted, such as viewing pornography or copying copyright protected materials, with which the customer is expected to comply. AUPs ‘tend to be used by organizations to pass some element of liability onto the customer when accessing internet services’ (McMenemy and Burton, 2005: 21). Goulding (2006: 197) found that the participants in her research (61 interviews with policy makers, strategists, senior public library practitioners and others with specific interests in
Filtering. Internet filtering software (sometimes referred to as content control software, content filtering software, censorware or web-filtering software) uses site blocking or keyword blocking or a combination of the two. According to McMenemy and Burton (2005) it is the ‘acceptable face of censorship’ and although librarians may not wish to employ it, they do so to comply with local authority policies. This state of affairs was echoed by Cooke (2006) who noted that decisions to implement filtering software in public libraries in the UK were often made at local authority level rather than by librarians themselves.

The disadvantages of filtering, which may block legitimate content (McMenemy, 2009) have emerged in a number of studies (see, for example, Sommerlad et al., 2004). McMenemy found, in a study of Internet access in UK public libraries using a ‘mystery shopper’ approach, that Internet filtering was inconsistent. He attempted to access a list of 25 different websites and found that two libraries blocked nothing on the list whilst others blocked some sites. Chat sites, an advice site for gay teenagers and a gambling site were the most commonly blocked. Some blocking was overt and some covert (McMenemy, 2008).

The exact number of PLAs in the UK utilising content control software is unknown. According to data from the NETbase Survey, administered by the PN team in late 2002, approximately 75% of respondents had installed filtering software at that time (86 of 210 PLAs responded to the survey) (Brophy, 2003).

Methods
As part of the overall research strategy for the MAIPLE project, a questionnaire was administered to PLAs. The survey was designed to ascertain the ways in which PLAs manage Internet access for the public, including the extent to which filtering is used, as well as other methods such as AUPs. Subsequent stages of the project will include case studies undertaken in at least four library services involving interviews with a number of staff and library Internet users.

The survey was designed and refined by the research team before a draft version was hosted online using Bristol Online Surveys (BOS). An email with a link to the online draft version of the questionnaire survey was sent to the members of the MAIPLE External Advisory Board in November 2012. They were asked to test it and to consider the appropriateness of the terminology used, whether there were any additional questions which should be included and if there was anything that ought to be removed. Three of the Board members tested the survey and emailed their comments to the researcher. The revised survey was then sent to three ‘critical friends’ of the MAIPLE project and an additional public library ICT manager to pre-test during December 2012. They received an information sheet detailing the background to the survey and its objectives. They were also asked to consider appropriateness, clarity and whether there were any obvious omissions. In addition, they were charged with considering whether the instructions regarding completion were clear and how long it took them to complete the questionnaire.

The subsequent refined questionnaire survey was hosted online using BOS. It consisted of 36 questions, divided into four sections, most of which used multiple choice buttons, with a small number of questions where respondents were asked to input text. Piloting of the questionnaire had indicated that it should take no longer than 15 minutes to complete. The project aimed to secure one response from each public library authority in the UK. An email was sent on 11 January 2013 to the appropriate senior library management contact held by the research team for every public library authority in the UK based on entries in Libraries and Information Services in the United Kingdom and the Republic of Ireland 2011–2012 (CILIP, 2012) inviting them or another relevant colleague to participate in the project.
by completing the survey. Unsurprisingly there were 15 undeliverable emails and the research team identified an alternative potential contact through the library service website or by telephoning the local authority and the survey invitations were re-sent. The first invitation had a closing date of 8 February 2013. Non-responders received two further email reminders politely encouraging participation. The survey finally closed on 22 February 2013. In total, 80 responses were received from a potential 206 services which represents a response rate of 39%. Survey data were cleaned and analysed in SPSS v.19 and are reported in the following section. In terms of country, 75.0% of respondents were from English public library services \( n=60 \), out of 151, 40%), 15.0% of responses were from Scottish authorities \( n=12 \), out of 32, 38%), 8.8% of responses were from Welsh public library services \( n=7 \), out of 22, 32%) and 1.3% were from Northern Ireland \( n=1 \), out of 1, 100%). ‘Total’ below refers to the total number of respondents answering that particular question. For some questions, respondents were able to select more than one option and in those instances percentages do not total 100. Almost half of respondents, 48.8%, defined themselves as senior library management \( n=39 \) whilst approximately one-fifth were middle management \( n=19 \) and library IT staff \( n=18 \) respectively.

### Findings

#### Decision making and the regulation of Internet access

Almost all of the responding services had an AUP for public Internet usage, \( n=79 \) (98.8%). One respondent did not know. In terms of the formulation of the AUP senior library service management were usually involved (88.6%) and in over half of responding services, library service IT staff were involved (57.0%). In just under half of responding services, the local authority’s IT team and/or legal staff were involved (46.8% and 45.6% respectively). Councillors (elected members) were involved in AUP formulation in fewer than 10% of services. ‘Other’ colleagues included Information Security staff. In around half of the responding services the AUP was signed off at senior library service management level (50.6%). Fewer services had their AUP signed off by the legal department of their local authority (13.9%), by local authority senior management (11.4%), by elected members (10.1%) or the IT department of the local authority (6.3%).

All 80 responding UK public library services provide filtered access to the Internet on all their PCs (100.0%). The decision to install filtering software (Table 1) appears to have been led by the IT departments of local authorities (26.3%), by library service senior management (25.0%) and by local authority senior management (22.5%). In three services, the decision to install filtering software had been a combined one involving more than one team, for example: ‘Decision was made by a working party of representatives from IT, IT Security and Library Service senior management’. In one service, use of filtering software had been a pre-requisite of the Internet Service Provider.

#### Overriding filtering software

In order to request a change in the filtering policy, library users may ask a member of staff in the library in approximately three-quarters of responding services (76.3%). In half of responding services Internet users can email a request to the library service (Table 2). Approximately one-fifth of services give users the opportunity to complete a form online (21.3%) or complete a paper form in the library (22.5%). Sixteen respondents selected ‘other’. Upon analysis of the comments submitted, in the majority of cases (13), a member of the public asks a member of library staff who then passes that request to colleagues in IT either within the library service or the local authority: ‘Make suggestion to staff in library who pass on the request to Corporate ICT’. One respondent noted that: ‘This is not an option’ in their service.
In 53 authorities, responsibility for responding to requests to change the filter rests with one particular group of staff (66.3%), but in 27 services it rests with more than one group (33.8%) of which 14 respondents selected two options (17.5%) and 10 respondents selected three options (12.5%). Library service senior management are involved in over half of responding services (52.5%). In approximately two-fifths of services library service IT staff (41.3%) and/or local authority IT staff (41.3%) are involved. Fewer than 10% of library services give frontline library staff any responsibility to respond to filtering change requests. Six respondents selected ‘other’. Their comments reveal that most of those involve staff with ICT responsibility including information security or virtual content. In one service, the IT service is outsourced to Capita, and filtering responsibility rests with them.

**Authentication of identity**

Respondents were asked what library members and non-members (guests) need in order to access the Internet in their libraries (Table 3). Almost all services require library members to have a library borrower number (98.8%). In 70 services, a PIN or password is required (87.5%). Of the respondents 70 (87.5%) indicated that library members require both a library borrower number and a PIN/password. A means of payment is only required by four services (5.0%).

For guests or non-members, half of responding services require some proof of identity (50.0%) whilst a PIN or password is required by almost half of responding services (47.1%). A quarter of responding services require a means of payment (25.0%). In five services, no authentication is required (7.4%).

Of those services responding ‘other’, five have some form of temporary ticket or log in for guests, for example: ‘Guests are logged in via a staff member using a guest “ticket”’. In two services, library members’ name and address details are required but not proof of these, although one service does post out a card to the address given and PC access is not permitted until the card is presented at the library. In one service, Internet users are issued with a library card for PC use only, which they may upgrade to borrow items.

More than four-fifths of the 80 responding library services (67 services, 83.8%) offer Wi-Fi access to the public at one or more of their libraries. To access Wi-Fi, a PIN or password is the most popular requirement of library members (61.2%) and of guests (50.0%) (Table 4). Almost half of responding services require library members to have their borrower number (49.3%) although in almost one-fifth of responding services, no authentication is required for library members (19.4%). For guests, proof of identity (28.3%) and no authentication required (26.4%) are also popular options. Of those selecting ‘other’, analysis of comments submitted reveals that requirements include an email address (5), adhering to the Wi-Fi supplier’s terms and conditions (4), a mobile telephone number (2), use of a guest card/log-in (2), accepting the AUP or Internet use policy (2), or setting up an account (1).

In approximately four-fifths of public library services (80.6%), Wi-Fi users see a special web page to log-on/authenticate before using the Internet, known as a captive portal (n=54, out of 67).

**Booking and/or charging measures**

Over 90% of responding services (n=73) use a proprietary software booking or reservation system giving users the opportunity to reserve, in advance, a time-slot on a library computer (92.4%). Three services do not have a booking system whilst one uses an in-house electronic system and another uses manual records. Over half of those using a proprietary booking system use Netloan by Lorensbergs (54.8%) whilst almost one-third use i-CAM by Insight Media Internet Limited (Table 5).

The Internet is free for everyone to use in 49 responding public library services (62.0%) (Table 6). In 19 services, there is a charge for visitors/non-members
Filtering and/or blocking measures

All 80 responding UK public library services provide filtered access to the Internet on all their PCs. Two-fifths of respondents use Websense filtering software (40.0%). Bluecoat was the second most popular filtering package used by nine services (11.3%) (Table 7).

Overwhelmingly, of the 67 responding services that provide Wi-Fi, the majority, n=56, provide filtered access to the Internet (83.6%). Eight services provide Wi-Fi that is unfiltered (11.9%) whilst three respondents did not know if their Wi-Fi provision was filtered or unfiltered. Over half of responding services provide secure Wi-Fi access – WPA or WPA2 (n=40, 59.7%); however, approximately one-quarter of respondents did not know (n=17, 25.4%) and 10 services do not provide secure access (14.9%).

Restricted content

Respondents were asked to indicate the content blocked by their filtering software by considering a list of 25 options drawn from a review of the literature and relevant filtering software websites during the desk research phase. Survey respondents had the option to select whether a particular category of content is blocked for ‘all users’, ‘only for children’ or ‘only for teenagers’ (Table 8).

The top five content categories blocked for all users are sexual (85.7%), hacking (83.1%), violence and intolerance/hate (both 80.5%) and extremist (79.2%). The least blocked content for all users are finance/banking (0%), social networking (1.3%), collaborative sites such as wikis (1.3%), blogs (3.9%) and personals/dating (5.2%).

Thirty-nine respondents (48.8%) block some content ‘only for children’. The top five content categories blocked for all users are sexual (85.7%), hacking (83.1%), violence and intolerance/hate (both 80.5%) and extremist (79.2%). The least blocked content for all users are finance/banking (0%), social networking (1.3%), collaborative sites such as wikis (1.3%), blogs (3.9%) and personals/dating (5.2%).

Thirty-nine respondents (48.8%) block some content ‘only for children’. The top five content categories blocked for all users are sexual (85.7%), hacking (83.1%), violence and intolerance/hate (both 80.5%) and extremist (79.2%). The least blocked content for all users are finance/banking (0%), social networking (1.3%), collaborative sites such as wikis (1.3%), blogs (3.9%) and personals/dating (5.2%).

Restricted content

Respondents were asked to indicate the content blocked by their filtering software by considering a list of 25 options drawn from a review of the literature and relevant filtering software websites during the desk research phase. Survey respondents had the option to select whether a particular category of content is blocked for ‘all users’, ‘only for children’ or ‘only for teenagers’ (Table 8).

The top five content categories blocked for all users are sexual (85.7%), hacking (83.1%), violence and intolerance/hate (both 80.5%) and extremist (79.2%). The least blocked content for all users are finance/banking (0%), social networking (1.3%), collaborative sites such as wikis (1.3%), blogs (3.9%) and personals/dating (5.2%).

Thirty-nine respondents (48.8%) block some content ‘only for children’. The top five content categories blocked for all users are sexual (85.7%), hacking (83.1%), violence and intolerance/hate (both 80.5%) and extremist (79.2%). The least blocked content for all users are finance/banking (0%), social networking (1.3%), collaborative sites such as wikis (1.3%), blogs (3.9%) and personals/dating (5.2%).

Thirty-nine respondents (48.8%) block some content ‘only for children’. The top five content categories blocked for all users are sexual (85.7%), hacking (83.1%), violence and intolerance/hate (both 80.5%) and extremist (79.2%). The least blocked content for all users are finance/banking (0%), social networking (1.3%), collaborative sites such as wikis (1.3%), blogs (3.9%) and personals/dating (5.2%).

Thirty-nine respondents (48.8%) block some content ‘only for children’. The top five content categories blocked for all users are sexual (85.7%), hacking (83.1%), violence and intolerance/hate (both 80.5%) and extremist (79.2%). The least blocked content for all users are finance/banking (0%), social networking (1.3%), collaborative sites such as wikis (1.3%), blogs (3.9%) and personals/dating (5.2%).

Thirty-nine respondents (48.8%) block some content ‘only for children’. The top five content categories blocked for all users are sexual (85.7%), hacking (83.1%), violence and intolerance/hate (both 80.5%) and extremist (79.2%). The least blocked content for all users are finance/banking (0%), social networking (1.3%), collaborative sites such as wikis (1.3%), blogs (3.9%) and personals/dating (5.2%).
Twenty-four respondents (30.0%) block some content ‘only for teenagers’. The top five content categories blocked for this age group are gambling and personals/dating (both 45.8%), weapons (29.2%), bad language (25.0%) and illegal drugs (20.8%) and the least blocked are instant messaging, RSS feed aggregators, file download/upload and webmail (all 0%).

Analysis showed that the comments provided for ‘other’ content blocked include live television (5) and child pornography (2). Two services had isolated specific sites for children: ‘All dedicated children’s PCs only provide access to selected ring fenced websites i.e. games and homework’. Other content mentioned as being blocked included school cheating information, historical revisionism and residential IP addresses.

Respondents were asked whether library users had made any complaints about the filtering software in the last 12 months. Almost two-thirds of respondents stated that they had received complaints (n=52, 65.8%) compared to 30.4% who had not (n=24). A small proportion of respondents did not know (n=3, 3.8%).

Of those services that had received complaints (n=52), over-blocking was the most frequent cause (88.5%) whilst the technical limitations of access such as the inability to upload or share files were also cited by over half of respondents receiving complaints (53.8%). Less numerous were complaints about the use of filtering software per se (19.2%). ‘Other’ complaints included users being unable to access online greetings cards, a drug-related website and access to Virtual Learning Environments (VLEs) (Table 9).

Respondents were asked their opinion of filtering. How useful did they judge it to be in maintaining acceptable Internet use in their libraries? Over half of all respondents judged it to be ‘very useful’ (n=45, 56.3%) and approximately two-fifths found it ‘somewhat useful’ (n=33, 41.3%). Only two respondents were negative about filtering, judging it to be ‘not very useful’ (2.5%).

### Expectations of use and information provided concerning content restriction

Public library Internet users are alerted to the AUP in a number of different ways. In over four-fifths of services, library users are made aware on the PC log-in screen (n=71, 89.9%) whilst in just under half of responding services, there is information on the library website (n=38, 48.1%). The AUP may also be highlighted on the PC/Internet use form (n=27, 34.2%), the library membership form/pack (n=22, 27.8%) and posters in the library (n=18, 22.8%). ‘Other’ ways include hand-outs in the library (two services) and ‘staff’, presumably making users aware of its existence.

In the majority of public library services, library users are made aware in the AUP that the library employs filtering software (n=71, 88.8%) (Table 10). Over half of responding services draw users’ attention to the use of filtering software when they log-on to the PC (n=45, 56.3%) and/or inform the public on the library website (n=41, 51.3%). 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’. In two services, users were notified electronically either by a message on the computer screen or at the point of filtering whilst paper hand-outs were used in one service.

### Other measures taken to regulate Internet use

The most commonly used measure, after filtering software and AUPs, to manage public Internet access is visual monitoring by library staff (83.5%) (Table 11). The positioning of PCs and use of a booking system are also popular mechanisms (70.9%). Collecting Internet use data is utilised by over two-fifths of respondents (44.3%) whilst monitoring software is used in almost a third of responding services (30.4%).

---

**Table 7. Filtering software package used.**

<table>
<thead>
<tr>
<th>Filtering Software Package</th>
<th>Frequency</th>
<th>Per cent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Websense</td>
<td>32</td>
<td>40.0</td>
</tr>
<tr>
<td>Bluecoat</td>
<td>9</td>
<td>11.3</td>
</tr>
<tr>
<td>Smoothwall</td>
<td>3</td>
<td>3.8</td>
</tr>
<tr>
<td>Netsweeper</td>
<td>3</td>
<td>3.8</td>
</tr>
<tr>
<td>Sophos</td>
<td>3</td>
<td>3.8</td>
</tr>
<tr>
<td>SurfControl</td>
<td>2</td>
<td>2.5</td>
</tr>
<tr>
<td>In-house solution</td>
<td>2</td>
<td>2.5</td>
</tr>
<tr>
<td>FortiGate</td>
<td>2</td>
<td>2.5</td>
</tr>
<tr>
<td>South West Grid for Learning</td>
<td>2</td>
<td>2.5</td>
</tr>
<tr>
<td>Bloxx</td>
<td>2</td>
<td>2.5</td>
</tr>
<tr>
<td>McAfee</td>
<td>2</td>
<td>2.5</td>
</tr>
<tr>
<td>Cisco</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>SmartFilter</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Dell SonicWALL</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>EZBN Protex</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>CLEO OneConnect</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Finjan (now M86 Secure Web Gateway)</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>IronPort</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Barracuda</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>RM SafetyNet Plus</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Trend Micro</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>WebMarshal</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Citrix</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Clearswift</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Atomwide</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Don’t know</td>
<td>4</td>
<td>5.0</td>
</tr>
<tr>
<td>Total respondents</td>
<td>80</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Table 9. Types of complaint about Internet filtering.

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Per cent</th>
<th>Frequency</th>
<th>Per cent</th>
<th>Frequency</th>
<th>Per cent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over-blocking, i.e. user unable to access legitimately required content</td>
<td>46</td>
<td>88.5</td>
<td>6</td>
<td>15.4</td>
<td>3</td>
<td>12.5</td>
</tr>
<tr>
<td>Technical limitations of access (inability to download/upload/file share)</td>
<td>28</td>
<td>53.8</td>
<td>5</td>
<td>12.8</td>
<td>3</td>
<td>12.5</td>
</tr>
<tr>
<td>Objection to use of filtering software</td>
<td>10</td>
<td>19.2</td>
<td>6</td>
<td>15.4</td>
<td>2</td>
<td>8.3</td>
</tr>
<tr>
<td>Other</td>
<td>6</td>
<td>11.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total respondents</td>
<td>52</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

‘Other’ additional measures include staff being vigilant, rather than visually monitoring Internet activity (in three services): ‘Staff will take action if they happen to see something but do not monitor usage’. Practical measures such as posters are used in one service: ‘Internet safety posters aimed at children and young adults’ whilst a volunteer-led programme called ‘computer buddies’, takes place in another service. Two services utilise technological measures such as adjusting the filtering categories whilst in one service, monitoring software is about to be introduced.

Table 10. Ways in which library users are made aware of Internet filtering.

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Per cent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable Use Policy</td>
<td>71</td>
<td>88.8</td>
</tr>
<tr>
<td>Log-in screen on PC</td>
<td>45</td>
<td>56.3</td>
</tr>
<tr>
<td>Information on the library website</td>
<td>41</td>
<td>51.3</td>
</tr>
<tr>
<td>PC/Internet use form</td>
<td>18</td>
<td>22.5</td>
</tr>
<tr>
<td>Posters in library</td>
<td>13</td>
<td>16.3</td>
</tr>
<tr>
<td>Library membership form/pack</td>
<td>13</td>
<td>16.3</td>
</tr>
<tr>
<td>Other</td>
<td>7</td>
<td>8.8</td>
</tr>
<tr>
<td>Total respondents</td>
<td>80</td>
<td></td>
</tr>
</tbody>
</table>

Special measures in place to protect minors from accessing inappropriate content

All the terminals in 77 PLAs (96.3%) have filtering software to protect minors (Table 12), defined as children and young people under 18 years of age in England, Wales and Northern Ireland and under 16 years in Scotland. In over half of responding services (n=43), minors access the
Internet in a dedicated area with oversight by staff (53.8%). Almost half of services rely on parental oversight of use (48.8%) and adherence to AUP (47.5%). In one-quarter of services, minors have dedicated terminals (25.0%). User education tailored to minors is used in 11 authorities (13.8%).

**Internet misuse**

Misuse incidents involving minors happen rarely according to approximately two-fifths of respondents (43.8%). It was reported by 30% of respondents that such incidents never happen (n=24) whilst in 12.5% of responding services, they sometimes happen (n=10). Eleven respondents did not know.

Approximately two-fifths of respondents thought that library users sometimes circumvented the Internet filter (n=33, 41.3%). However, around one-third perceived that it rarely happened (n=27, 33.8%). Around one-fifth of respondents did not know (n=17, 21.3 per cent) and three thought that it never happened (3.8%). None thought it was a frequent problem.

‘Major’ breaches of the AUP (examples of which were not stipulated in the questionnaire) are known to occur ‘rarely’ (n=30, 38.0%) and ‘sometimes’ (n=25, 31.6%) in the majority of responding authorities. According to 10 respondents, breaches ‘never’ happen (12.7%) whilst in 14 services, the respondent did not know (17.7%). The largest proportions of respondents felt that ‘minor’ breaches of the AUP (again, examples were not specified in the questionnaire) ‘rarely’ happened (n=34, 43.0%) or ‘sometimes’ happened (n=31, 39.2%). Ten respondents did not know (12.7%).

Overwhelmingly, ‘major’ and ‘minor’ breaches were considered to be the result of library users viewing obscene (legal and illegal) content (82.2% and 92.7% respectively) (Table 13). Viewing racist, extremist or hate content as a ‘major’ breach of the AUP was noted in six services (13.3%) whilst viewing violent content was judged as a ‘minor’ breach in nine services (16.4%). Fewer than 10% of responding services ‘major’ and ‘minor’ AUP breaches involved hacking (8.9% and 3.6% respectively), criminal activity (4.4% and 3.6% respectively) or spamming (1.8% in each case). ‘Other’ ‘major’ breaches (four) include damage to equipment, users attempting to log-in with other users’ details and inappropriate user behaviour whilst ‘other’ ‘minor’ breaches include attempts to change PC settings and the booking system, viewing unacceptable materials sent via email or on social networking sites, streaming TV, using other people’s log-in details and unacceptable behaviour.

**Managing access to the Internet – what works well?**

Respondents to the MAIPLE survey were asked to describe what they feel works particularly well with regard to managing public access to the Internet in their services, and 58 did so. The comments submitted were analysed thematically and the results are presented in Table 14. Use of filtering software and an electronic booking system for Internet use emerged as the most popular options to manage Internet access.

**Discussion**

These preliminary results suggest that PLAs manage public access to the Internet in similar ways relying on a number of complementary mechanisms to ensure users’ identity may be authenticated and traced if required. Users typically need to be a member of the library to use the Internet, evidenced in a membership card and PIN number, although guests/non-members may also access the Internet. Their
Table 13. Types of major and minor AUP breaches.

<table>
<thead>
<tr>
<th>Major</th>
<th>Frequency</th>
<th>Per cent</th>
<th>Minor</th>
<th>Frequency</th>
<th>Per cent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing of obscene (legal and illegal) content</td>
<td>37</td>
<td>82.2</td>
<td>51</td>
<td>92.7</td>
<td></td>
</tr>
<tr>
<td>Viewing of violent content</td>
<td>4</td>
<td>8.9</td>
<td>9</td>
<td>16.4</td>
<td></td>
</tr>
<tr>
<td>Viewing of racist, extremist or hate content</td>
<td>6</td>
<td>13.3</td>
<td>6</td>
<td>10.9</td>
<td></td>
</tr>
<tr>
<td>Online bullying/harassment</td>
<td>5</td>
<td>11.1</td>
<td>6</td>
<td>10.9</td>
<td></td>
</tr>
<tr>
<td>Malware/viruses</td>
<td>3</td>
<td>6.7</td>
<td>6</td>
<td>10.9</td>
<td></td>
</tr>
<tr>
<td>Copyright infringement</td>
<td>2</td>
<td>4.4</td>
<td>6</td>
<td>10.9</td>
<td></td>
</tr>
<tr>
<td>Hacking</td>
<td>4</td>
<td>8.9</td>
<td>2</td>
<td>3.6</td>
<td></td>
</tr>
<tr>
<td>Criminal activity</td>
<td>2</td>
<td>4.4</td>
<td>2</td>
<td>3.6</td>
<td></td>
</tr>
<tr>
<td>Spamming</td>
<td>1</td>
<td>1.8</td>
<td>1</td>
<td>1.8</td>
<td></td>
</tr>
<tr>
<td>Other breaches</td>
<td>4</td>
<td>8.9</td>
<td>5</td>
<td>9.1</td>
<td></td>
</tr>
<tr>
<td>Total respondents</td>
<td>45</td>
<td>55</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 14. Respondents’ views of what works well in relation to managing public Internet access.

<table>
<thead>
<tr>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filtering software</td>
</tr>
<tr>
<td>Booking system</td>
</tr>
<tr>
<td>AUP/policy</td>
</tr>
<tr>
<td>Monitoring (software and staff oversight)</td>
</tr>
<tr>
<td>Library Management System</td>
</tr>
<tr>
<td>Location of PCs</td>
</tr>
<tr>
<td>Relationships/communication e.g. with IT staff</td>
</tr>
<tr>
<td>Action/ban</td>
</tr>
<tr>
<td>Staff support/training</td>
</tr>
<tr>
<td>Wi-Fi</td>
</tr>
<tr>
<td>Training for users</td>
</tr>
<tr>
<td>Publicity</td>
</tr>
<tr>
<td>Free access</td>
</tr>
<tr>
<td>Charging for use</td>
</tr>
<tr>
<td>Time limits on usage</td>
</tr>
<tr>
<td>Total respondents</td>
</tr>
</tbody>
</table>

presence on a PC is usually logged in a commercially available booking system and their ability to look at content is proscribed by the content permitted by the filtering software. Their activity may be randomly checked by software or by the physical presence of library staff monitoring behaviour visually.

**Wi-Fi and the rise in use of mobile devices to access the Internet**

However, there is some evidence from the survey data that there are still decisions to be made in relation to the management of wireless Internet access. The results indicated that for those responding PLAs, all static PCs with Internet access were filtered and yet not all Wi-Fi provision was subject to content control mechanisms. In addition, there were some loopholes for visitors wishing to use the Internet and Wi-Fi connections, whereby verification of identity was not always required.

Indeed, the growth of Wi-Fi availability in public libraries is pertinent to the successful management of Internet access. Data indicate that the percentage of adults in Great Britain who have accessed the Internet in public libraries has fallen from 10% in 2006 to 4% in 2010 (ONS, 2010). In contrast, the percentage of adults accessing the Internet using a Wi-Fi hotspot increased from 2% in 2007 (ONS, 2008) to 7% in 2010 (ONS, 2010). The growth in availability and ownership of hand-held and portable devices which provide mobile Internet access suggests that Wi-Fi availability and management in public libraries will be an on-going issue. According to the Office for National Statistics (ONS, 2011: 2): ‘Mobile Internet use via a laptop, tablet or other portable computer also proved popular in 2011, with 38 per cent of Internet users using these mobile devices away from the home or workplace’. This had increased from 18% in 2007 to 26% by 2009 (ONS, 2009) rising up to 38% by 2011 such that by 2012, 58% of adults had used portable computers and handheld devices to access the Internet ‘on the go’ in the last three months (ONS, 2013).

There are certainly data to indicate that Wi-Fi availability in UK public libraries is increasing. A report undertaken by a commercial Wi-Fi provider based on a survey carried out in 2008 and 2009 discovered that of the 92 responding PLAs, 47% had already implemented Wi-Fi, 28% were planning to implement Wi-Fi and 25% were not currently planning Wi-Fi installation (Insight Media Internet Limited, 2009). Our survey results reveal that more than four-fifths of responding library services offer Wi-Fi access to the public at one or more of their libraries. This appears to confirm Batt’s (2009) assertion based on the results of three surveys of public library Wi-Fi activity between 2006 and 2009, that there was a significant increase over that period of Wi-Fi provision by public libraries.
The majority of the 67 services in our survey that offer Wi-Fi provide filtered access to the Internet (83.6%). This is similar to the results of a survey by Insight Media Internet Limited in 2009, which found that for 84% of PLAs, the hotspot provided filtered access to the Internet and for 67% of PLAs this filtering would be the same as the PN filtering rather than separate (33%). In terms of security, over half of responding services in our study, provide secure Wi-Fi access – WPA or WPA2 (59.7%); however, approximately one-quarter of respondents did not know (25.4%) and 10 services did not provide secure access (14.9%). Batt (2009) reporting the results of the National WiFi in Libraries Survey 2009, found that 27% of responding PLAs thought encryption was in place, 29% did not and 44% did not know.

To access Wi-Fi, almost half of responding services require library members to utilise their borrower number (49.3%). Batt (2009) cites two surveys from 2009 which questioned whether users were required to identify themselves with the Library Management System (LMS) checking their details. Around one-third of libraries with Wi-Fi were using the LMS to authenticate users. Our findings indicate that PLAs are increasingly using the LMS to authenticate Wi-Fi users. However, as our results also reveal, in some PLAs, guests are accessing Wi-Fi without being authenticated via the LMS. This issue was highlighted in 2009 by Insight Media Internet Limited which asked PLAs to reflect on the journey to Wi-Fi installation:

> It would appear that some audit departments expect the same user authentication and audit trail information from Wi-Fi implementations as they do from the People’s Network applications, where users are commonly using their borrower credentials to access the service. This information then provides access to services, providing a detailed audit trail of activity and utilisation. Some solutions allow users to access Wi-Fi without adhering to these procedures and therefore cannot provide such an audit trail. (Insight Media Internet Limited, 2009:28)

**The effectiveness of filtering, AUPs and other Internet management tools**

The MAIPLE study is considering all the available mechanisms by which public libraries may successfully manage acceptable and legal Internet access by the public. One tool, albeit a controversial one, is the use of filtering software which ‘seeks to keep a user from finding or viewing certain types of material’ (Diaz, 1999: 147). In the USA, the American Library Association and American Civil Liberties Union have both been vocal in their opposition to filtering (Bertot et al., 2010). Similarly, in the UK, the Chartered Institute of Library and Information Professionals (CILIP) states in its guide to user privacy in libraries that: ‘CILIP does not endorse the use of filtering especially for adult users but recognises that a number of libraries do use filtering systems especially if it is required by their parent institution’ (CILIP, 2011: 12). However, our survey results suggest that the use of filtering software is rather more widespread in UK public libraries than CILIP estimated. Similarly, research in Scotland recently found that 31 of 32 PLAs used filtering software (Brown and McMenemy, 2013). Our results also indicate that library staff perceive filtering software as successful in managing acceptable Internet use in their libraries. When asked how useful respondents judge filtering to be, over half of respondents decided it was ‘very useful’, and approximately two-fifths found it ‘somewhat useful’. Only two respondents were negative about filtering, judging it to be ‘not very useful’.

CILIP suggest that if filtering is used in a public library it should be acknowledged and that the public have the opportunity to request the unblocking of sites: ‘Where filtering is in operation, is this acknowledged publicly? Does the library have an override capability so as to respond to users’ requests to unlock specific sites? Can users appeal against inaccurate filtering? Do some terminals provide unfiltered access?’ (CILIP, 2011: 12–13). In more than half of responding services users were made aware of filtering software, conspicuously, each time they logged-on to the PC. Less conspicuously, it might be argued, was the use of the AUP as the tool by which the majority of responding PLAs made users aware of filtering (or informing the public on the library website that Internet content is filtered). A small minority of services did not specifically make users aware of Internet filtering, and only one indicated that unblocking sites at the request of users was not an option in their PLA. In contrast, in the USA, adults may request not only that a site is unblocked but that filtering is turned off or disabled. According to the American Library Association (2013), ‘libraries must turn off the filter upon request by an adult, without inquiring into the adult’s “purpose” for disabling the software’.

Analysis of the comments made by respondents regarding successful management of Internet access saw the emergence of Internet booking systems as a popular tool. Over 90% of responding services used a software booking system of which over half used Netloan by Lorensergs, confirming McMenemy’s (2009) observation that a popular choice of booking systems for public access PCs was Netloan, which requires the library barcode number and PIN as it interfaces with the LMS data to authenticate the computer user.

AUPs remain an important tool in managing Internet access and breaches of the AUP were mostly judged to be infrequent. This was Brophy’s (2003) conclusion a decade ago: ‘The statistical data so far available suggests that problems in this area are relatively rare, with most authorities reporting AUP violations in single figures. However, it is an area which needs to remain under continuous monitoring’. When breaches did occur, the respondents in our
survey indicated that they were overwhelmingly related to library users viewing obscene content. Indeed, it is difficult to locate with ease any information relating to copyright breaches by the public when using the Internet in public libraries whilst information about users convicted of viewing child pornography, for example, is more widely available (FBI, 2012; Britton, 2011). The viewing of ‘obscene’ content is, in itself, contestable, as definitions of obscenity are many and variable. Content that to one person could be deemed to ‘tend to deprave and corrupt’ (Great Britain, 1959: 1) might be considered relatively harmless and innocuous to another.

**Making decisions about Internet access and its implications for staff**

Our survey results revealed that decision making in relation to Internet access is generally in the hands of library service senior management when it comes to the AUP and the decision to install filtering software. Where it may differ is the responsibility to respond to and make a change to the filtering of content following a request from a member of the public. Local authority IT personnel may also make this decision. In 27 services, more than one group of staff was responsible for making decisions about filtering.

Less than one-fifth of respondents indicated that public library staff receive regular Internet training. This contrasts with the findings of a report to the Museums Libraries and Archives Council based on an online survey to which 112 English PLAs responded (CFE, 2010). They found that 72% of PLAs’ frontline staff had received digital training since undertaking their PN ICT training.

**Conclusion**

The MAIPLE survey aimed to establish a quantitative overview of measures being taken in public libraries across the UK with regard to the provision and regulation of public Internet access. All responding libraries are using filtering software to regulate this access, although the 39% response rate should suggest caution in the interpretation of these findings – perhaps those authorities who take more proactive measures towards content regulation were more inclined to respond or this topic area is one which professionals struggle to discuss openly. Nevertheless, these findings are broadly in line with those found in Scotland by Brown and McMenemy (2013) who reported 31 out of 32 PLAs using filtering software. We were also interested in establishing where the responsibility for decision making with regard to the employment of filtering software lies – in this respect, it is noteworthy that in most instances this appears to rest with senior library management rather than local authority management. Ownership of procedures for ‘unblocking’ access to legitimate sites appears to be more diverse; but it is reasonable to conclude that the bureaucratic nature of such processes and the resultant privacy loss will deter many users from making such requests in the first place.

Procedures for authentication of identity for static Internet access appear more uniform, and it can be deduced that public libraries have the means to know who is using their facilities and, in most cases, to trace back any misuse to individual users. Whether such procedures have been accompanied by any privacy impact assessment is an area that warrants further research. Wi-Fi access appears to be a rapidly growing, but much less regulated infosphere in public libraries; however, it can be speculated that this is a case of technology advancing faster than bureaucracy can keep pace with, and it is likely that more stringent authentication measures will follow in due course. Indeed, the role of technology can be seen to be important here, as a few large companies were found to dominate the market for solutions to public library access, whether it be filtering (e.g. Websense Inc.) or booking control (e.g. Lorensbergs). From a technologically determinist perspective, it can be speculated that these external companies wield considerable power in the shaping of public access to the Internet in libraries – again, this area deserves further academic attention.

Sexual/obscene content appears to be that which causes greatest concern and that is most likely to be restricted, closely followed by other potentially illegal categories such as hate-speech and other extremist content. However, given that the Internet Watch Foundation already acts at national level as a regulatory body to screen out access to material determined to be illegal, it is possible that much more than illegal content is being withheld from library users. The lack of transparency on the part of the filtering software providers makes it difficult to determine where the boundaries are being drawn with regard to the upholding of community standards (Boyce, 2008), and it is clear that these judgments are not generally in the hands of professional librarians. However, whilst the most common cause of complaint about filtering software from library users related to over-blocking, it does have to be acknowledged that a large majority of respondents (97.6%) found the software useful in helping them to manage public Internet access.

Public libraries were also found to rely on a range of other measures to prevent misuse of public Internet access facilities, including AUPs, overt and covert monitoring of use and training of users. More restrictive measures are often in place for access by children and young people, including, in some cases, the provision of dedicated terminals with access to specially selected sites only or ‘walled garden’. The fact that incidents of misuse appear to be relatively rare could be seen to be evidence of the success of measures taken; an over-estimation of the size of the problem in the first place; or perhaps that public library staff are simply not aware of misuse that takes place. There is scope for further research here.
Overall, it can be concluded that the combination of measures that are currently in place to regulate public Internet access in UK public libraries is having some success in ensuring that public use remains legal and within the boundaries of common acceptability. The use of filtering software appears to be a generally accepted and popular solution. What is less clear is the extent to which users are being denied legitimate ‘access to all publicly available information’ as far as resources allow (CILIP, 2005), as decreed by the professional body and code of ethics to which information professionals aspire.

Acknowledgements
The authors would like to thank Sharon Fletcher, LISU for administering the online survey and Sonya White, LISU for undertaking the preliminary analysis of the survey results. The advice provided by the MAIPLE External Advisory Board and critical friends during testing and piloting is also much appreciated. We would like to thank all the survey contacts and respondents who gave their time to participate. Finally, the comments of the reviewers were greatly appreciated.

Funding
This work was supported by the Arts and Humanities Research Council (AHRC) [grant number AH/J005878/1].

Notes
1. The remit of the ‘critical friends’ (professionals in the field suggested to the project by Advisory Board Members) is:
   - To contribute relevant subject and professional expertise, knowledge and guidance via virtual communication;
   - To contribute ideas and debate to ensure the achievement of best possible project outcomes for all stakeholders;
   - To scrutinise and provide critical feedback on relevant project documents and outcomes;
   - To assist with dissemination of project findings beyond academia.


References


Author biographies

Dr Rachel Spacey is Senior Research Associate, LISU, Loughborough University. Rachel’s research interests include public libraries; learning in museums, libraries and archives; and the benefits of reading for pleasure.

Dr Louise Cooke is Senior Lecturer in the Centre for Information Management at Loughborough University. She is also Director of Postgraduate Studies, as well as MSc Information and Knowledge Management Programme Leader. Her research interests include the regulation of public Internet access in libraries and social and digital inclusion.

Claire Creaser is Director, LISU, Loughborough University. Claire Creaser has been employed at LISU since 1994, and was appointed Director in 2007. Her main areas of interest are in the use of statistical evidence for the management of libraries and information services, with a particular focus on benchmarking; analysis and interpretation of survey data; and scholarly communication, including open access to research outputs.

Dr Adrienne Muir is Senior Lecturer in Publishing in the Department of English and Drama, Loughborough University. Her research interests include information and publishing law, policy and ethics and preservation of intellectual heritage.