Managing access to the internet in public libraries [MAIPLE]

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


Additional Information:

- This report is also available to download free of charge at: http://www.lboro.ac.uk/microsites/infosci/lisu/maiple/pubs.html

Metadata Record: https://dspace.lboro.ac.uk/2134/17645

Version: Published

Publisher: LISU, Loughborough University (© Loughborough University)

Rights: This work is made available according to the conditions of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) licence. Full details of this licence are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Please cite the published version.
Managing Access to the Internet in Public Libraries

[MAIPLE]

August 2014

Report written by:
Rachel Spacey and Louise Cooke with Adrienne Muir and Claire Creaser
Managing Access to the Internet in Public Libraries [MAIPLE]

End of Award Report Submitted to the Arts & Humanities Research Council
Grant: AH/J005878/1

Principal Investigator: Louise Cooke
Researcher: Rachel Spacey
Co-applicants: Adrienne Muir
Claire Creaser
Administrative support: Sharon Fletcher


© Loughborough University
ACKNOWLEDGEMENTS

The MAIPLE team would like to thank:

External Advisory Board members past and present
Jeannette Castle (Chair)
John Dolan, OBE
Guy Daines
Chris Batt, OBE
Alan Poulter
Martin Molloy, OBE
Prof. Anne Goulding

Critical Friends
Phil Jones
Richard Veevers
Sue Lawson

Survey
All the respondents who kindly completed the questionnaire; Valérie Spezi, LISU for additional help with the project and Sonya White, LISU for survey analysis.

Case Studies
The staff that helped set up the visits and all the staff and users who agreed to be interviewed.

Workshop
Prof. Anne Goulding
Jeanette Castle
Ayub Khan, MBE
Darren Smart
Brian Ashley

Plus all the participants who contributed to the debates and discussion.
# CONTENTS

**EXECUTIVE SUMMARY** ........................................................................................................... iv

**INTRODUCTION** ........................................................................................................................ 1
  - Background ........................................................................................................................................ 1
  - Aims and objectives ........................................................................................................................... 1
  - Research Questions .......................................................................................................................... 2
  - Limitations of the research ................................................................................................................ 2
  - Structure of the report ....................................................................................................................... 2

**METHODS** ................................................................................................................................. 3
  - Introduction ........................................................................................................................................ 3
  - External Advisory Board .................................................................................................................... 4
  - Critical Friends ................................................................................................................................... 5
  - Literature Review ............................................................................................................................... 5
  - Survey ................................................................................................................................................ 5
  - Case Studies ...................................................................................................................................... 6
  - Workshop ........................................................................................................................................... 9

**REVIEW OF THE LITERATURE** .............................................................................................. 10
  - Introduction ...................................................................................................................................... 10

**RESULTS** ............................................................................................................................... 25
  - Survey .............................................................................................................................................. 25
  - Case Studies .................................................................................................................................... 44
  - Case Study Data Analysis ............................................................................................................... 72
  - Public WiFi in the UK: Desk Research ............................................................................................ 81
  - Workshop ......................................................................................................................................... 86

**DISCUSSION** ........................................................................................................................... 87

**CONCLUSIONS** ....................................................................................................................... 91
  - Reflections on research limitations ................................................................................................... 94

**RECOMMENDATIONS** ............................................................................................................ 96

**OUTPUTS** ................................................................................................................................... 98

**IMPACTS** ................................................................................................................................... 99

**FUTURE RESEARCH** ............................................................................................................... 100

**BIBLIOGRAPHY** ..................................................................................................................... 101

**APPENDIX 1: Questionnaire survey** ....................................................................................... 110

**APPENDIX 2: The Workshop** .................................................................................................. 119

**APPENDIX 3: Filtering of WiFi hot spots** ................................................................................ 122
LIST OF TABLES AND FIGURES

Table 1  Case study chronology ................................................................. 8
Table 2  Filtering software package used .................................................. 31
Table 3  Categories of sites blocked for all users, only for children and only for teenagers .... 33
Table 4  Types of major AUP breaches ...................................................... 39
Table 5  Types of minor AUP breaches ...................................................... 40
Table 6  Respondents’ views of what works well in relation to managing public Internet access ......................................................... 43

Figure 1  Methods used in the MAIPLE project ........................................... 3
Figure 2  Geographical response by country ............................................... 25
Figure 3  Job category of respondents ....................................................... 25
Figure 4  Requirements for Internet access on a library PC ......................... 26
Figure 5  Booking system for PC use ......................................................... 27
Figure 6  Charges for Internet access ......................................................... 27
Figure 7  Requirements of users in order to access WiFi .............................. 28
Figure 8  Is WiFi access filtered? ................................................................. 29
Figure 9  Is WiFi access secure? ................................................................. 29
Figure 10  Captive portal ............................................................................ 30
Figure 11  Decision to install filtering software .......................................... 30
Figure 12  How to Request a change in the filtering policy ............................ 34
Figure 13  Responsibility for responding to filter change requests ............... 34
Figure 14  Ways in which library users are made aware of Internet filtering .... 35
Figure 15  Complaints about the Internet filter ............................................ 35
Figure 16  Types of complaint about Internet filtering .................................. 36
Figure 17  Opinions of the usefulness of filtering ....................................... 36
Figure 18  Perception of the frequency of filter circumvention by users ........... 37
Figure 19  Staff involved in the formulation of service’s AUP ....................... 37
Figure 20  Staff involved in signing-off the AUP ........................................ 38
Figure 21  Ways in which library users are alerted to the AUP ...................... 38
Figure 22  Major breaches of the AUP ....................................................... 39
Figure 23  Minor breaches of the AUP ....................................................... 40
Figure 24  Additional measures ................................................................. 41
Figure 25  Do Staff receive regular Internet training? ................................. 41
Figure 26  Measures to protect minors using the Internet ............................ 42
Figure 27  Frequency of incidents involving minors and misuse .................... 42
EXECUTIVE SUMMARY
Managing Access to the Internet in Public Libraries (MAIPLE) was a 24-month project funded by the Arts and Humanities Research Council (AHRC), carried out between September 2012 and August 2014 by a team from Loughborough University, led by Dr Louise Cooke.

The aim of the project was to identify measures taken in UK public libraries to regulate access to Internet content, and evaluate their impact and effectiveness. A mixed methods approach was adopted comprising a review of relevant academic, professional and grey literature; an online questionnaire survey of Public Library Services with 80 responses; five in-depth case studies of public libraries across the UK; desk research into commercial public WiFi provision; and a workshop for a range of stakeholders, held towards the end of the project to test and refine the findings. The team was supported throughout by an independent External Advisory Board of experts in the field.

Key findings from the research include:

- Filtering of Internet access appears to be ubiquitous in UK public libraries, with 100% of survey respondents reporting that their public access is filtered to a lesser or greater degree.
- Librarians generally accept filtering as a pragmatic solution to the regulation of public Internet access, albeit with some reluctance.
- There is a lack of transparency with regard to filtering, with around half of users interviewed in the case studies unaware that access was filtered.
- Users were generally supportive of decisions concerning the filtering of access in libraries, particularly where children were concerned.
- Decisions concerning filtering policy appeared to have been taken either by senior personnel within the library service or by senior IT personnel in the relevant local authority.
- Procedures for unblocking sites on request are inconsistent, and around half of users interviewed would be uncomfortable asking library staff to unblock a site, however legitimate the site may be.
- The majority of library services have an Acceptable Use Policy (AUP) in addition to filtering software.
- Major breaches of the AUP are rare; minor breaches are most frequent in relation to viewing pornographic material.
- Levels of staff training vary, and staff interviewed felt that more formal training to keep up to date would be welcomed.
- Commercial public WiFi providers operate a diverse set of criteria with respect to filtering, which often depend on the policies and preferences of the company mediating public access.

The project findings support the conclusions of previous research with regard to the ubiquity of filtering and suggest that its popularity has grown over the lifespan of the People’s Network. Librarians appear to be at risk of marginalisation from key decision-making in this area, which is often devolved to IT or local government managerial personnel, and even (and perhaps more worryingly) the vendors of Internet Service Provision. What is clear from the findings is that access to legitimate Internet content is being withheld from users on a seemingly arbitrary basis, often for reasons of simple expediency.

Nevertheless, it appears that most library personnel and users are satisfied with the status quo, and accept that the public library’s symbolic representation as a ‘decent public space’ carries with it necessary restrictions on access to Internet content. Issues of privacy were also found to exist, with users’ access taking place in a ‘virtual panopticon’ of surveillance measures. Whilst other measures, such as the use of an AUP, were found to be in place, they were not being implemented very effectively, with most users unaware of their content, despite having signed up to the policy.
The advent of WiFi is posing new challenges, and public libraries find themselves having to adopt similar measures to commercial providers with regard to content restriction. Given that many of the users we spoke with were suffering from multiple disadvantage (e.g. unemployment, benefit dependency etc.), it is disappointing to note that they also had to contend with the challenges posed by measures to manage Internet access in public libraries. These include time limits on use that were insufficient to prepare and submit a job application. Other measures that have the potential to combat digital and social inclusion such as the teaching of digital skills were often left to volunteers, who themselves did not always possess the level of skills necessary to take on this role effectively.

A summary of our key recommendations is as follows:

1. Any content filtering in place for material accessed by adults should be set at the lowest possible level for all categories of material (excepting illegal content such as child pornography, which should be blocked at source);
2. Adult content should not be restricted to the level deemed appropriate for minors. Wherever possible, a separate area should be provided for use by minors so that the risk of inadvertent viewing of content more suited to adults is minimised.
3. Content accessed by minors may be subject to more stringent restrictions, but should still not impose undue levels of censorship.
4. There should be a simple, transparent and effective mechanism for having sites unblocked, that demonstrates respect towards the individual user. Library personnel should receive appropriate training and authority in the unblocking of sites, so that patrons are not prevented from accessing legitimate content.
5. There is a need for much greater transparency and openness about the use of filtering. Patrons and library personnel should always be aware of content restrictions in place, and the rationale for their imposition.
6. Much greater attention needs to be paid to education and training both of patrons and library personnel. Those responsible ‘on the ground’ for oversight of use of public library Internet use should receive appropriate (and regular) training, so that they are in a position to support and inform patrons with regard to acceptable use, and any measures in place to facilitate this. Library users, and in particular minors, would benefit from greater attention being paid to their own education with regard to the retrieval of useful and appropriate content, and in staying safe online.
7. Surveillance and monitoring of patrons’ use of the Internet should also be kept to the absolute minimum necessary to ensure legal compliance. In addition, all patrons should be made aware of any surveillance measures in place, whether these are real-time monitoring of screens or the potential for retrospective scrutiny of web browsing histories.
8. There is a need for more professional debate on the topic in the light of professional ethical commitments to freedom of access to information.
9. There is a need for a more unified and consistent approach to managing Internet access based on nationally agreed guidelines.
10. Above all, it should be widely recognised that public library Internet facilities are a highly valued service, and that they should be fully promoted and extended, particularly with regard to the provision of WiFi access.
INTRODUCTION

Background
This end of project report summarises the work of the Managing Access to the Internet in Public Libraries [MAIPLE] project, funded by the Arts and Humanities Research Council, Grant: AH/J005878/1.

MAIPLE was undertaken by a team from the Centre for Information Management (Dr. Louise Cooke), LISU (Dr. Rachel Spacey, Claire Creaser and Sharon Fletcher) and the Department of English, Drama and Publishing (Dr. Adrienne Muir) at Loughborough University in the following roles:

Principal Investigator: Dr. Louise Cooke
Co-Investigators: Dr. Adrienne Muir and Claire Creaser
Research Associate: Dr. Rachel Spacey
Administrative support: Sharon Fletcher

MAIPLE, a 24 month project, commenced in September 2012 and finished in August 2014.

Aims and objectives
The introduction of public Internet access into UK public libraries has been important in generating greater equality of access to information for UK citizens and has enabled significant steps to be taken in the provision of electronic public services (e.g. the ability to renew driving licences or pay Council Tax online). This offers considerable potential benefit to both government and the citizen, in terms of cost-savings, accessibility, democratic participation and environmental sustainability. However, the provision of Internet access in public libraries has also led to concerns that such access would lead to misuse and the downloading of inappropriate and illegal content (Cooke, 2004; Home Office, 2011).

A very limited amount of research had previously been undertaken that provided a comprehensive picture of measures taken in the UK to address these concerns, or of the effectiveness and impact of alternative approaches. MAIPLE aimed to identify and quantify measures implemented in UK public libraries to regulate and manage access to Internet content. MAIPLE also aimed to investigate the adoption of technical measures, such as filtering software, and organisational measures, such as Acceptable Use Policies (AUPs) and the provision of user education and evaluate their impact and effectiveness. In order to meet its aims, the following objectives were identified for the project:

1. To collect and analyse comprehensive quantitative data relating to the extent of implementation of filtering software, AUPs and other measures in UK public libraries in order to manage and regulate access to Internet content;
2. To collect and analyse comprehensive qualitative data concerning the management and regulation of access to Internet content in UK public libraries, from the perspective of library personnel, managers and users;
3. To collect and analyse comprehensive qualitative data concerning the management and regulation of wireless access to Internet content by commercial providers such as cafes as a benchmark for comparison and the exchange of good practice;
4. To identify a model for practice in public libraries with regard to the provision of Internet access that will provide a financially, legally and ethically sustainable solution that can be adapted easily to the changing technological landscape;
5. To produce a set of guidelines for UK public librarians to assist them in managing the provision of public access to the Internet whilst remaining within the boundaries of legal, ethical and practical constraints;
6. To provide relevant knowledge and guidance to professional bodies such as CILIP in order that they may offer strong leadership, advice and support grounded in empirical knowledge and evidence to those charged with the provision of public Internet access;
7. To identify examples of good practice in managing public access to the Internet for all user groups in UK public libraries;
8. To identify, through desk and empirical research, all legal, ethical and public policy measures that impact on the provision of public access to the Internet in UK public libraries;
9. To analyse the effectiveness and functionality of different filtering software solutions;
10. To disseminate, test and refine results in a workshop for project stakeholders.

Research Questions

1. What measures are used by public libraries to regulate Internet content access, and how extensive are they?
2. What are the problems, if any, raised by these measures for those charged with managing public Internet access?
3. Is there any impact on the library user's freedom of access to information as a result?
4. How effective are the measures in regulating access to inappropriate or illegal content?
5. How could the management of public Internet access be improved to ensure stronger legal compliance without impacting adversely on freedom of enquiry?
6. Are minors (i.e. those under 18 in the UK) being adequately protected from online dangers such as predatory adults or exposure to adult content?
7. Are the measures currently being taken the most cost-effective available, or are there more cost-effective solutions that could be adopted?
8. How can librarians prevent the infringement of copyright that results from clients’ downloading or file-sharing activities?
9. What specific problems have arisen for public libraries as a result of the advent of social media (e.g. social networking sites), and how are these currently being addressed?
10. How can public librarians be protected from legal liability as a result of their clients' actions?
11. What lessons can local authorities learn from practice elsewhere including from the commercial provision of public Internet access?
12. What additional benefits (if any) does free, public, supported Internet access in public libraries confer above commercial provision?

Limitations of the research

The online questionnaire was undertaken in 2013 and the response rate was approximately 40 per cent. Five case studies were also undertaken. A case study ‘allows the researcher to deal with the subtleties and intricacies of complex social situations’ (Denscombe, 2003, p.38, italics in original), but can make generalisations difficult. However, a case study can be a useful method for theory-building and theory-testing, and our case studies proved useful and valid in this context.

Structure of the report

This report details the methods used to gather data (Methods) followed by a Review of the Literature. The Results are then presented including those of the online questionnaire survey and the case studies. A Discussion is followed by Conclusions and Recommendations. The Outputs of the MAIPLE project are detailed and its impacts considered. Future research questions are suggested. Finally, a Bibliography and Appendices are presented.
METHODS

Introduction

MAIPLE has employed a mixed methods approach using tools which generate both quantitative and qualitative data. This enabled the research team to examine the issue in a number of different ways. At the beginning of the project an External Advisory Board (EAB) was established which provided expert knowledge throughout the course of the research. A literature review was undertaken when the project commenced to help inform the research questions to be explored in the survey and case study stages. Critical friends of the project were individuals highlighted by the EAB as those in the profession who could provide additional sectoral insight. The three critical friends helped critique the questionnaire used in the online survey, which was disseminated to all 206 public library services in the UK. Following the survey, case studies were carried out building upon the survey results. The interview questions asked of staff and users in the case studies were derived from the literature review, the survey results and the contributions of the EAB and project team. An additional piece of desk research was undertaken in year two of the project to further inform the findings in relation to public WiFi provision. The data generated from the interviews undertaken as part of the case studies was analysed using NVivo 10, a qualitative data analysis (QDA) computer software package. To further refine and validate the findings of the MAIPLE project, a workshop was held on July 10th 2014 with key personnel relevant to the field invited to comment on the draft findings and recommendations.

Figure 1  Methods used in the MAIPLE project
External Advisory Board

The External Advisory Board was established in September 2012. The first meeting was held on September 11th 2012 and was chaired by Prof. Anne Goulding. A number of relevant issues and suggested publications were discussed which were followed up in the desk research phase. The second meeting took place in March 2013 and was chaired by Jeannette Castle, Library and Heritage Services Coordinator, West Lothian Council. Subsequent meetings were held in September 2013, March 2014 and July 2014.

The remit of the External Advisory Board was agreed at the first meeting:

1. To attend and contribute to five bi-annual Board meetings;
2. To monitor progress of the project against the project objectives and work plan;
3. To contribute relevant subject and professional expertise, knowledge and guidance;
4. To contribute ideas and debate to ensure the achievement of best possible project outcomes for all stakeholders;
5. To scrutinise and provide critical feedback on relevant project documents and outcomes;
6. To disseminate and communicate project findings to the world beyond academia.

Members:

Prof. Anne Goulding – Formerly, Reader in the Department of Information Science at Loughborough University, author of Public Libraries in the 21st Century (Ashgate, 2006) and editor of Journal of Librarianship and Information Science. Anne initially chaired the Advisory Board before relocating to New Zealand.

Jeanette Castle – Library and Heritage Services Coordinator, West Lothian Council. Jeannette has been responsible for the strategic leadership of the library and heritage services of West Lothian Council for almost a decade. She is a management board member of the Scottish Library and Information Council and is an Elected Councillor on the CILIPS Council. Jeanette chaired the Advisory Board following Anne’s departure.

Chris Batt, OBE – Senior Research Fellow at University College London and independent consultant to the public sector on the use and impact of digital technologies. Until 2007 Chris was Chief Executive of the Museums, Libraries and Archives Council (MLA) and led the implementation of the highly successful £170 million People’s Network project that enabled the deployment of Internet access in public libraries.

Guy Daines – Head of Policy at the Chartered Institute of Library and Information Professionals (CILIP). Guy is responsible for professional policy development at CILIP and has a keen interest in the issue of Internet filtering in libraries. He also has responsibility for CILIP’s Ethical Principles and legal issues relating to information.

John Dolan, OBE – Head of Community Regeneration at Eye, Honorary Research Fellow in the Department of Information Studies at Aberystwyth University and CILIP Trustee (2011-2014). John was awarded his OBE for services to Libraries and Information Provision. His past roles include Head of Library Policy at MLA and Assistant Director (Learning) at Birmingham City Council.

Martin Molloy, OBE – Formerly Strategic Director, Cultural and Community Services, Derbyshire County Council. Martin has served in a variety of professional roles, including Chair of the Board of the Reading Agency, Board member of the East Midlands MLA, and member of the Advisory
Committees of the Departments of Information Studies and Information Science at the Universities of Sheffield and Loughborough respectively. He is a past President of CILIP, a past President of the Society of Chief Librarians, a past member and past Chair of the Advisory Council for Libraries, and past Chair of the DCMS Libraries and Adult Learning Steering Group.

**Alan Poulter** – Lecturer in the Department of Computer and Information Sciences at Strathclyde University, Alan has long been interested in issues around public Internet access. Previous research includes the Frills project (Forensic Readiness for Local Libraries in Scotland), which aimed to develop simple, low-cost techniques to provide a basic readiness regime for public access ICT facilities. He is co-author of *A Handbook of Ethical Practice: a Practical Guide to Dealing with Ethical Issues in Library and Information Work* (Chandos, 2007), and of *The Library and Information Professional’s Internet Companion* (Facet, 2005).

**Critical Friends**
The role of the three ‘critical friends’ was:

1. To contribute relevant subject and professional expertise, knowledge and guidance via virtual communication;
2. To contribute ideas and debate to ensure the achievement of best possible project outcomes for all stakeholders;
3. To scrutinise and provide critical feedback on relevant project documents and outcomes;
4. To assist with dissemination of project findings beyond academia.

The three were:

- **Phil Jones**, Academic Liaison Librarian at the University of Worcester (The Hive);
- **Richard Veevers**, Frontline Library Officer, Lancashire County council;
- **Sue Lawson**, Service Development Coordinator, Information and Digital, Manchester City Council.

**Literature Review**
Desk research commenced September 2012. This involved a comprehensive, critical analysis of secondary sources relating to the issue of Internet access in public libraries in the UK and internationally, including any available statistical material and qualitative analyses. It also included reviews of any current guidance on the issue available from national, international and supra-national bodies.

The initial literature review was completed by December 2012. It was used as the basis of a journal article which was published in the *Journal of Documentation* in 2014 [see Output]. The review confirmed that there is a lack of academic study with regard to Internet regulation in public libraries in the UK and that the issue of filtering of content on public access computers is highly contentious and merits further study. The literature review has been updated throughout the course of the MAIPLE project.

**Survey**
The online questionnaire survey was designed to elicit a picture of how UK public library services are managing Internet access. This element of the study was intended to collect factual data with regard to the extent of implementation of filtering software and other regulatory measures. Desk research had helped identify other questionnaires used in similar studies as a basis for comparison.

The questionnaire consisted of an Introduction which set out the background to the survey. It also informed respondents that there were 36 questions in four sections. Section 1 asked questions
about the background of the respondent; Section 2 considered Internet access; Section 3 asked questions about how that access is managed and Section 4 asked respondents about their willingness to be involved in the next stage of the research. A copy of the final questionnaire is included at Appendix 1.

Pre-test, piloting and distribution
The online questionnaire was drafted and refined throughout December 2012 and January 2013. The link to the draft of the online survey was distributed to the six members of the External Advisory Board with a request to try it out and consider the terminology used, any additional questions to be asked and whether any items should be removed. Three members of the group emailed the researcher with their comments, the majority of which were incorporated. Some were of a technical nature and others related to terminology.

Following the pre-test, the second draft of the online pilot was completed and was issued with instructions on completion to eight individuals known to the research team who currently or recently worked in public libraries in a variety of posts including the three ‘critical friends’ of the project. Detailed responses were received from three of the eight invited to take part in the pilot. Their comments were incorporated into the third draft of the questionnaire. Pilot volunteers were asked to consider whether the instructions on the Introduction were clear; if the questions were clear and appropriate; if there were any other questions which might be asked and how long it took to complete the questionnaire.

The survey was hosted online using Bristol Online Surveys [BOS]. An email was sent on January 11th 2013 to the appropriate contact held by LISU for every public library service in the UK inviting them or another relevant colleague to participate in the project by completing the survey. Non-responders received two further email reminders. The survey finally closed on Friday 22nd February 2013.

Response rate
In total, 80 responses were received from a potential 206 services which represents a response rate of 39 per cent.

Data analysis
Survey data were cleaned and analysed in SPSS v.19 by Sonya White, LISU Assistant Statistician. The results were then written up by Rachel Spacey, LISU Senior Research Associate, and shared with the MAIPLE team.

The survey phase was completed by the end of April 2013. It was used as the basis of a journal article which was published in the Journal of Librarianship and Information Science [see Output].

Case Studies
The case studies were designed to enable the identification of good practice, lessons learnt and transferability of practice such as AUP policy development. The case studies involved a combination of analysis of policy documents and other relevant material; interviews with key stakeholders such as IT managers and library personnel; and interviews with users. Twenty four survey respondents had expressed a willingness to participate in this phase of the research. Cases were selected from these on the basis of convenience and purposive sampling, taking into account participants’ geographical location, size and library sector. Representative public library services from all four home countries of the UK participated in the case studies.
Case study sites were approached via an email to the online survey respondent. We explained that the case studies were an opportunity to explore some of the issues which emerged in the survey data in detail and to share good practice. We anticipated that each case study visit would consist of the following:

**Pre-visit**
- Documentary analysis
- A telephone interview (if relevant)

**Visit (possibly over 1 - 3 days depending on staff availability)**
- An interview with a senior manager
- An interview with a member of IT staff
- An interview with at least one member of front line staff
- Brief interviews with library Internet users (our aim was to achieve up to six user interviews in each case study site)

**Post-visit**
- We sent a draft of the case study for approval prior to publication.

We also explained that individual case study reports will be made available on the project website as well as being incorporated into the final project report. No individuals would be identified in published documents.

**Interviews**
Documentation produced as part of the case study investigations included participant information forms and consent forms for both staff and user interviewees. We also drew up schedules of interview questions for users and for staff. For the latter there were some slight variations including some different questions for management and for frontline staff to reflect on their differing responsibilities in relation to the public using the Internet.

**Issues covered**
Interview schedules for managers included a section on their role (background); managing access – filtering, acceptable use policy and misuse; staff; education and training; and changing use. Questions for front line staff included a section on background; supporting public access to the Internet; managing access; education and training; and changing use. Interview schedules for users consisted of background; accessing the Internet; using the Internet; filtering; and future usage.

**Sampling**
On the basis of volunteers willing to put their PLS forward as potential case study sites and consideration of geographical location, five sites were eventually selected and agreed to participate in the study. Two PLS were in England, one in Scotland, one in Wales and Libraries NI. PLS varied in size ranging from four libraries (case study 5) to almost 100 (case study 2).

**Transcription**
All the interviews with staff and users were recorded with their permission and handwritten notes made. Following the visits the audio recordings were transcribed and cleaned. The transcripts were then used to inform the writing of the case study.
The five case studies completed were:

**Case study 1 – Derbyshire, England.** A visit to Chesterfield Library was undertaken in April 2013. Six members of staff at different organisational levels within Cultural and Community Services, the department which includes library services, were interviewed: Assistant Director, Service Relationship Manager, Senior Librarian, Access and Inclusion Librarian, Assistant Library Manager and Library Assistant. Four members of the public volunteered to take part and were interviewed in situ.

**Case Study 2- Edinburgh, Scotland.** Researchers visited Central Library, City of Edinburgh Council in May 2013 where they interviewed seven members of staff at different organisational levels within the library service which sits within Services for Communities. Interviewees were the Digital and Information Services Manager, two Team Leaders and four Library Advisors. Six members of the public volunteered to take part and were interviewed in situ.

**Case Study 3 – Brighton & Hove, England.** In June 2013, researchers visited two of Brighton & Hove’s libraries: Jubilee Library and Hove Library where they interviewed four members of staff at different organisational levels within City Services the department which includes Brighton & Hove Libraries. Interviewees were a Library Community Engagement Manager, ICT Consultant, Library Officer and Safety and Security Officer. In addition a telephone interview took place with the Head of Service prior to the visit. Five members of the public volunteered and were interviewed in situ at Hove Library.

**Case Study 4 – Libraries NI, Northern Ireland.** Researchers visited one of Libraries NI’s Regional Admin Centres and a branch library in September 2013 where they interviewed six members of staff at different organisational levels within Libraries NI. Interviewees were an Operational Manager, Project and Service Manager and Project Officer at the Admin Centre and two Branch Library Managers and Library Assistant at a local branch library. Six members of the public volunteered to take part and were interviewed in situ.

**Case Study 5 – Merthyr Tydfil, Wales.** Researchers visited Merthyr Tydfil Central Library in Wales in November 2013 where they interviewed seven members of staff at different organisational levels within Merthyr Tydfil County Borough Council. Interviewees included an Operations Librarian, Assistant Librarian, two Member Support staff, two Library Assistants and a Desktop Services Engineer. Six members of the public volunteered to take part and were interviewed in situ.

All the interviews were recorded and later transcribed. Five draft case studies were written by the project team and shared with the respective case study contact for approval.
Data analysis
The interview transcriptions were also analysed together using qualitative analysis software, NVivo10. This was to consider specific themes and issues which emerged from the interviews with both staff and users as a whole in addition to the individual case study narratives.

Further desk research
During the proposal writing stage of the MAIPLE project it had been planned to undertake a case study with an Internet café provider. Once the project began it became clear in discussion with the External Advisory Board that the landscape had changed somewhat with the rise in popularity of cafés with wireless Internet access [WiFi]. It was judged that research into this arena would provide fruitful comparative data with which to compare developments in public libraries. The sixth case study therefore became a piece of desk research based on a thorough search of the literature available in the public domain on the Internet and in academic journals in relation to commercial outlets providing WiFi. Consideration was made of a number of well-known commercial outlets that a user might reasonably come across in a UK city, such as Costa Coffee, Pizza Express and Virgin Trains.

Workshop
An invitation-only end-of-project workshop was scheduled as a means to share some of the project findings and to elicit feedback on the reliability of our findings from key members of the public library community. It was held on July 10th 2014 at Burleigh Court, Loughborough University. The day consisted of a keynote speech delivered by Prof. Anne Goulding who had been the initial chair of the MAIPLE EAB. The MAIPLE team then presented the results of the project and break out groups discussed some of the key issues. The discussions were recorded and transcribed and incorporated into the final results. A panel was convened which held a debate on some of the pertinent issues.

A report of the day and the recommendations made can be found at Appendix 2.
REVIEW OF THE LITERATURE

Introduction
A comprehensive search of the literature from the last 15 years (1997-2012) was initially undertaken to inform the literature review. Sources were located through electronic databases including Library and Information Science Abstracts (LISA) and Zetoc as well as Internet searches. Relevant sources were also highlighted by the project advisory group. The literature review was kept updated throughout the course of the project.

More than 100 relevant academic and professional journal articles, monographs, reports, theses, news articles, guidance and publications have been identified and reviewed. These are detailed in the bibliography for this report.

Research exploring Internet access in public libraries and its management in the UK is numerically small and dates mostly from the beginning of the 21st century; see, for example, Willson & Oulton (2000). There has, however, been some relatively recent research mapping WiFi availability in public libraries (Batt, 2009) and in relation to public Internet access in Scottish public libraries (Brown & McMenemy, 2012).

This review considers the historical background to Internet access in public libraries in the UK and details the research available. It also considers the legal duties public libraries must adhere to in relation to the public accessing the Internet. Sources relating to Internet access in public libraries internationally are also detailed. The research relating to examples of misuse is explored, followed by arguments both for and against the use of technical measures such as filtering software identified in the literature. Organisational measures to manage Internet use are also identified.

Internet access in UK public libraries: background
Computers have been available in public libraries in the UK since the 1960s, although not necessarily for the use of the public but in back room operations such as cataloguing, library circulation systems and online databases. Throughout the 1970s and 1980s a range of borrowing services were automated and by the 1990s, Information Technology (IT) in libraries included library management systems for staff and facilities designed for the public including PCs to access CD-ROMs, undertake word processing and surf the Internet (Spacey, 2003). Developments in public libraries in the UK in the mid to late 1990s were stimulated by a number of government strategies during a period of advancement of the concepts of lifelong learning, increasing IT use (by which point it was now commonly referred to as ICT (Information and Communication(s) Technology/ies)) and reducing social exclusion. Most notable of these were New Library: The People’s Network published in 1997 by the now defunct Library and Information Commission, the government’s response to this paper in 1998, and Building the New Library Network (LIC, 1998). Funding of £100 million was committed to provide the infrastructure to connect all static library points to the Internet, which became known as the ‘People’s Network’ and £20 million was allocated to train all public library staff in the United Kingdom (Goulding, 2006). At present, public libraries in the UK provide a range of services to their communities of which computers with Internet access is just one. However, over the last decade this function has become crucial as “public libraries have featured large in government initiatives to extend Internet access beyond those connected at home or through work” (Goulding, 2006:167). Internet access in public libraries provides a means for those without Internet access at home or work to access commercial and governmental services and information. Data collected in relation to the percentage of adults in Great Britain who have accessed the Internet, for example, in the National Statistics Omnibus Survey.
reveal that an estimated 10 per cent of adults accessed the Internet in a public library in 2006, falling to four per cent in 2010 (ONS, 2010a; ONS, 2010b). In that same time period, accessing the Internet at home has increased from 85 to 95 per cent of adults whilst visiting an Internet café has decreased from eight to three per cent. Unfortunately, figures from 2011 do not include public libraries or Internet cafés. However, other data indicate that public library Internet access and use has increased. Dutton & Blank found that the percentage of current Internet users using the public library to access it increased from five per cent in 2003 to 15 per cent in 2011 compared with the percentages using Internet cafés which increased from three per cent in 2003 up to nine per cent in 2007 and fell to eight per cent in 2011 (Dutton & Blank, 2011:10). According to the charity Go On UK, there are 16 million adults in the UK without the basic online skills to benefit from the web (Go On UK, 2012).

Public libraries in the UK currently provide Internet access through 43,365 terminals (CIPFA, 2012) offering a potential 83,436 hours of usage of the People’s Network PCs (of which, 35,819 hours were recorded as having been used) with over 4,434 service points (2011-2012)\(^1\). There were 909 service points in England, 103 in Wales, 171 in Scotland and 3 in Northern Ireland in 2012 providing WiFi access. Many public libraries also provide varying levels of ICT support and training for members of the public. The government’s ‘assisted digital’ approach to supporting those who do not use digital services at present has been developed with input from organisations including the Society of Chief Librarians and stipulates that it will build on the support already provided to members of the community to use the Internet by public libraries:

“As the default, assisted digital support will be provided through the private sector, wider public sector providers such as libraries or local government, and the voluntary and community sector” (Cabinet Office, 2012:10).

Public libraries provide public access to the Internet within the law and issues of digital copyright must be considered.

**Research on managing Internet access in public libraries in the UK**

Willson and Oulton (2000) reported the results of a questionnaire survey, part of the public places, private spaces (PuPPS) project which looked at privacy, anonymity and confidentiality in public libraries, funded by the Library and Information Commission (1999-2000). Responses were received from 111 Public Library Authorities (PLAs) in England, Scotland and Wales. The survey explored Internet access, policy and controls, including software.

In terms of controls, they found that 71 per cent of PLAs imposed some form of control on public access terminals, with filtering the most popular mechanism (52 per cent). However, the study showed that problems arose as a consequence of filtering, including too much blocking with users unable to access legitimate sites. PLAs were questioned about controls on both public access and staff only PCs. Controls were more prevalent on public access PCs (71 per cent compared with 56 per cent of staff-only PCs) 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 per cent) followed by blocking controls (23 per cent) and monitoring (16 per cent).

Policies relating to electronic content were more directly and publicly accessible in the form of AUP posters near Internet terminals compared to policies relating to print materials which were often

\(^{1}\) There are 151 local authorities in England, 32 in Scotland, 22 in Wales and one in Northern Ireland (Libraries NI).
included in mission statements or stock selection policies. Those in favour of controls were usually concerned with sexually explicit and/or racist material being accessed. Those against the use of controls would perhaps have them on the PCs in the children’s library whilst PCs in public areas were visible and became self-regulating.

Goulding considered the People’s Network programme in the UK which included the roll out of infrastructure and public library staff training to enable staff to support public library users wishing to access the Internet. She cites research which explored public library staff’s attitudes to the Internet including concerns about users accessing inappropriate material: “Spacey (2004) found that filters and firewalls installed to prevent this created their own aggravations. As well as slowing the system, staff also had to deal with annoyed users who could not access legitimate material which had been stopped by a filter” (2006:197). Goulding found that the participants in her research (61 interviews with policy makers, strategists, senior public library practitioners and others with specific interests in public libraries) “were concerned about the policing of acceptable use of the facilities” but overall, “many study participants took a liberal attitude in relation to the use of People’s Network facilities, although some were having to revisit their AUPs in the light of experience” (2006:197).

In the UK, 14 different library authorities were visited by a researcher using a ‘mystery shopper’ approach - eight in England, four in Scotland and two in Wales (McMenemy, 2008). Of those 14, 12 allowed the researcher access to the Internet although the researcher was not a resident and did not have any identification which included address. In just one of those 12 libraries, staff attempted to explain the AUP and in two of them staff logged onto the computer for the researcher and bypassed the AUP. The author found 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 was covert.

Research was undertaken by a commercial WiFi provider in 2008-9 to review and evaluate WiFi services in public libraries in the UK (Insight Media Internet Limited, 2009). The first stage of the research involved contacting each PLA in the UK to identify an appropriate contact to respond to the questionnaire. Completed questionnaires were received from 92 PLAs (43 per cent of all PLAs). Of these 47 per cent had already implemented WiFi, 28 per cent were planning to implement WiFi and 25 per cent were not currently planning WiFi. A higher proportion of PLAs had implemented WiFi in England compared to other parts of the UK. The majority of services were implementing WiFi as a library service initiative rather than a local authority driven plan (79 per cent). The majority of PLAs provided or were going to provide WiFi for library members and guests. For 67 per cent of PLAs who had WiFi installed, this was using the existing infrastructure of the People’s Network (PN), of those planning WiFi, 69 per cent were going to use the PN. For 84 per cent of PLAs, the hotspot provided filtered access to the Internet and for 67 per cent of PLAs this filtering would be the same as PN filtering rather than separate (33 per cent).

“It would appear that some audit departments expect the same user authentication and audit trail information from WiFi 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 WiFi without adhering to these procedures and therefore cannot provide such an audit trail” (Insight Media Internet Limited, 2009:28).

Batt (2009) considered data in relation to WiFi in public libraries from three sources and noted that there had been a significant increase of WiFi provision by public libraries over the period 2006 to
in 2009. This provision was free in the main in 2006 (90 per cent of respondents) and in 2009, no respondents charged for WiFi. Between half and two thirds had linked their WiFi service into the pre-existing PN infrastructure (this was asked in the two studies from 2009). The 2009 surveys also questioned whether users were required to identify themselves with the LMS checking their details. Around a third of libraries with WiFi were using the LMS to authenticate users. The National WiFi in Libraries Survey 2009 asked if WiFi signals extended beyond the library (hot spots) – 30 per cent were aware that the signal did reach beyond the library. Twenty-eight of 61 libraries with WiFi hot spots required user name and password (45 per cent). In relation to security, 27 per cent thought encryption was in place, 29 per cent did not and 44 per cent did not know. A captive portal, which forces a client on a network to see a special web page which is usually used to highlight library services and news before they are able to access the Internet was present in 71 per cent of libraries.

Purdie, Williams & Tyler’s 2010 survey exploring use of Web 2.0 technologies by public library staff via heads of Welsh public library services, with a 60 per cent response rate, found that social networking and instant messaging were the most blocked types of site. Approximately 40 per cent of public libraries blocked access to social networking; RSS feed aggregators, blogs and Twitter, tagging and social bookmarks, instant messaging and multi-media file sharing. Less than 30 per cent of public libraries blocked access to collaborative sites such as wikis. Responsibility for restricting access (generally for staff rather than the public) was usually an organisational one (81 per cent); organisation and library (14 per cent) or library (five per cent). Restrictions were justified on the basis of security, organisational policy, the safety of children, bandwidth, and misuse of work computers during work hours, inappropriate content (e.g. staff blogs) and distractions from work.

The fifth report in the Oxford Internet Survey series investigating Internet access in Great Britain in 2011 based on a sample of 2,000 people with a response rate of 51 per cent found that half of all users access the Internet over their phone (49 per cent). Almost one-third of Internet users had a reader or tablet: “Fully 59% have access to the Internet via one or more of these multiple devices other than the household personal computer” (Dutton & Blank, 2011:4). They define ‘next generation users’ (NGUs) as “someone who accesses the Internet from multiple locations and devices...someone who uses at least two Internet applications... on their mobile or who fits two or more of the following criteria: they own a tablet, own a reader, own three or more computers” (Dutton & Blank, 2011:4). In 2011, “44.4% of Internet users in Britain were next generation users” (Dutton & Blank, 2011:5). They found that NGUs tend to have higher incomes and are more likely to produce content rather than simply consume it e.g. creating a profile on a social networking site, posting messages, videos, and stories or maintaining a blog. There are still a proportion of people who do not use the Internet – “Internet use in Britain grew from just over 60% in 2003 to 73% in 2011”. In terms of accessing the Internet in public libraries, 19 per cent of NGUs compared with 12 per cent of first generation users access it in the public library (Dutton & Blank, 2011:6).

Accessing the Internet on a mobile device has risen from 20 per cent of all users in 2009 to 40 per cent in 2011. There is no gender difference in accessing the Internet in public libraries. However, men are more likely to access the Internet in Internet cafes (10 per cent of men compared to seven per cent of women): “Libraries, on mobile devices, and another person’s home tend to be more important for people with lower incomes, whereas work and home access are more common among the higher income groups” (Dutton & Blank, 2011:10).

Brown & McMenemy detail the findings of research based on 32 Scottish public library authorities who responded to Freedom of Information requests (Brown & McMenemy, 2013). Of the 32 authorities, 31 reported that they use filtering software. Of these 31 authorities, 24 used filtering software ‘to prevent access to illegal and/or inappropriate content’; the second most common reason, cited by nine authorities was ‘to protect children and vulnerable users from inappropriate
material’. In terms of the organisational level at which policies were implemented, in 18 local authorities the decision was made by external senior management, in seven it was a management team within the library service, in five it was a joint decision between library and external management and in one they did not know. In the majority of authorities (27) there was a ‘release procedure’ in place but it was not immediate for content blocked by the filter. In 18 local authorities there was no training for staff relating to Internet filtering whilst six authorities did offer training. In one authority there was training for nominated staff and in five it was included in their general staff training. The content of staff training was primarily the procedure for blocking/unblocking content (10). Staff in six authorities were trained in the relationship between Internet filtering and the AUP.

In terms of accessing the Internet outside the home, the authors cite Ofcom research from 2008 which noted that 12 per cent of 8-17 year olds accessed the Internet in the library (Byron, 2008:102). With regard to UK policy on online crime prevention, the Prevent strategy is part of the counter-terrorism strategy, CONTEST, and was launched in 2007 and refocused in 2011. In this, the Internet is identified as a means by which terrorist individuals and organisations can reach and interact with a wider audience. Measures to curtail online radicalisation include “limit access to harmful content online in specific sectors or premises (notably schools, public libraries and other public buildings)” (HM Government, 2011:77). However, the command paper goes on to state that “We do not yet have a filtering product which has been rolled out comprehensively across Government Departments, agencies and statutory organisations and we are unable to determine the extent to which effective filtering is in place in schools and public libraries” (HM Government, 2011:79).

International comparisons

USA

Since much of the literature identified is American in origin, we shall begin with the situation in the USA. The management of Internet access in public libraries in the USA is shaped to some extent by legislation. In December 2000, the Children’s Internet Protection Act (CIPA) was signed into law. CIPA requires schools and libraries providing computers with Internet access to use a technology protection measure (TPM) to protect children against accessing visual depictions in child pornography, obscenity and harmful material (C-O-H), if they are to be eligible for federal subsidies towards the cost of Internet access, known as ‘e-rate’ funding. TPMs include filters, blocking specified sites determined by the library or ‘blacklists’; allowing specified sites approved by the library or ‘whitelists’; and Platform for Internet Content Selection (PICS) which allows web page creators to classify their own sites (Minow, 2004).

The constitutionality of CIPA was challenged by the American Library Association but “On June 23, 2003, the U.S. Supreme Court, in a 6-3 ruling, declared the Children’s Internet Protection Act constitutional” (Sobel, 2003:3). The CIPA requirements for adults differ, as material that is considered harmful to minors is not restricted as a matter of course for adults. Since adult users may request unblocking of their access, TPMs should offer the feature to disable - turning the entire filter off - and/or unblock individual sites. On this basis, the Supreme Court dismissed concerns about CIPA’s constitutionality: “The Court assumed that librarians would automatically and unconditionally disable filters upon request by adult patrons and permanently unblock erroneously blocked sites” (Sobel, 2003:15).

In 2012, a district court held that the North Central Regional Library District’s filtering policy did not violate the US constitution. The suit had been filed by the American Civil Liberties Union (ACLU) of Washington in 2006 alleging that the library violated the First Amendment by refusing to disable
blocking software at the request of adult library users. The district court’s decision was based on the premise that because branch libraries are small and only one library has a partition separating the children’s area from the rest of the library, the library’s refusal was justified (Chmara, 2012). In contrast, the US District Court for the Eastern District of Missouri held in February 2012 that the school district had unconstitutionally blocked websites that support/advocate on behalf of lesbian, gay, bisexual and transgender people whilst permitting access to websites that condemn homosexuality. The school district was fined and has to submit to monitoring for 18 months. Chmara notes that these decisions do not change the rules on filtering in the USA: “If libraries use filters that block constitutionally protected material deemed harmful to minors and do not allow adults to disable filters, or fail to provide an effective unblocking system, those libraries may open the door to years of litigation and significant legal expenses” (Chmara, 2012:3).

The number of public libraries in the USA who use technical measures such as filtering software to manage public Internet access is well documented. Since 1994, a national survey of USA public libraries has tracked the escalation of public library Internet access. Formerly known as the Public Libraries and the Internet study series, this research is now conducted as part of the larger annual Public Library Funding and Technology Access Study. Over the course of the last 18 years, the data reveal that the number of libraries using filtering software has increased. According to Jaeger & Yan (2009), almost all public schools in the USA and half of public libraries have implemented the requirements of CIPA. On the other hand, a rising and significant proportion of urban public libraries do not apply for e-rate funding precisely because they do not wish to comply with the stipulations of CIPA (Bertot et al, 2012). For example, it was reported that the number of libraries who considered the CIPA requirements unacceptable had increased by 15.3 per cent from the 2006 survey to 33.9 per cent of a sample of 6,979 libraries with 4,027 responses (Bertot et al, 2008). As a result public libraries in poorer parts of the country are more likely to have filtered access (McClure et al, 2007).

Canada
Dupelle noted that the last piece of research to ascertain whether Canadian public libraries used Internet content filters was published in 2001: Curry & Haycock found that 21 per cent of public libraries used filtering software but only 5 per cent used it on ALL their terminals (Dupelle, 2007).

Australia
The Australian Library and Information Association’s survey of public libraries and Internet filtering (2007) received responses from 104 out of a potential 548 services. Approximately 39 per cent of respondents noted that their library used Internet filtering software on some or all of its public Internet access terminals. Two earlier surveys of Internet use in public libraries which included some similar questions had found this to be 31 per cent in 2005 and 18 per cent in 2002. More recent figures suggest that approximately one third of libraries – 37 per cent – are now using Internet filter software whilst 61 per cent did not (similar to percentages from the 2005 and 2008 studies). For 41 per cent of those filtering this was done at a low to medium level whilst 32 per cent of libraries who filtered access did so at a higher level. In the main this was to filter offensive content although other filtered items included large files, file sharing, games and social networking sites.

Africa
A questionnaire sent to public libraries in ten English-speaking sub-Saharan African countries supported by the Carnegie Corporation of New York revealed that of the 22 services responding, 19 library services had access to the Internet. Ten services indicated that they controlled access whilst 12 tracked the URLs visited by users (Chisenga, 2004). The numbers involved in this study render it difficult to draw generalizable conclusions, but provide the only current indication of the prevailing
situation in sub-Saharan Africa: further work in this region would be very beneficial to provide a wider picture.

**Denmark**
A study in Denmark based on a questionnaire survey of 243 public library systems (PLS) with a response rate of more than 83 per cent, found that only two per cent of PLS had installed filtering software on their public access computers; while seven per cent were considering it (Pors, 2001). This comparatively relaxed approach to the provision of public Internet access offers a suggestion as to the impact of national cultures on decisions concerning filtering, with the example of a traditionally more liberal Scandinavian country appearing less likely to filter access.

**Russia**
In 2002, Trushina undertook questionnaire research which received responses from 25 Russian regional libraries of different types (public and research) to explore opinions of filtering. She found that Russian public libraries installed filters to prevent access to pornography and to suppress chat and e-mail. On occasion libraries were motivated to have a filter in place to ease “possible traffic congestion” (Trushina 2004:419).

**Other international**
Hamilton’s 2004 thesis funded by the International Federation of Library Associations (IFLA) and the Royal School of Library and Information Science in Copenhagen, surveyed national library and information professional associations and asked whether the association was in favour of filtering information on library Internet terminals, whether filtering was widespread in libraries and the motivations for filtering. Of 84 countries answering, 52 per cent were not in favour of filtering, six per cent were in favour and 42 per cent were in favour to a certain degree. Filtering was widespread in nine per cent of countries’ libraries, to a certain degree in 27 per cent and not widespread in 64 per cent of countries’ libraries. The response involves a subjective assessment of what is ‘widespread’ but of those 42 associations whose countries did have widespread filtering of the Internet the motivations included the protection of children (35), to safeguard public morality (20), to prevent criminal activity (10), to safeguard national culture (6), to protect national security (5), to safeguard religious values (4) and ‘other’ which included virus protection, pornography and safeguarding servers (3).

**Is Internet misuse really a problem?**
Internet misuse is frequently defined as viewing harmful content, primarily, pornography. Although Colaric cautions that access to pornography is not the only concern library staff should have about public access to the Internet: “the Web is also replete with incomplete information, pranks, contradictions, out-of-date information, improperly translated data, unauthorized revisions, factual errors, biased information, and scholarly misconduct” (2003:6). Curry’s (2000) study in Canada analysed 5000 transaction logs on seven public access workstations, equating to one week’s use of the Internet, in Burnaby Public Library, British Columbia. Terminals were unfiltered and protected by privacy screens. Curry found that most sites visited were related to communication (e.g. webmail), web communities, business and information: use of sexually related sites both soft and hard-core was limited possibly because most of the sites required membership using credit card details. Curry concluded “It appears that customers accessing these sites are either not members or are unwilling to enter their membership names in a public terminal. Most sites were accessed as ‘quick peeks’ in between much longer e-mail sessions or within information searching sessions” (2000:45). An article in an American professional journal for library staff (Oder, 2008) discussed research from a local newspaper which suggested 7.5 per cent of pages viewed during one 45 minute window contained pornography in the Dallas Public Library. Sitting alongside other research the author
Managing Access to the Internet
in Public Libraries [MAIPLE]

suggested this percentage seemed rather high as the Chicago Public Library had reported less than five per cent of traffic was to sexually explicit web sites in 1999.

A recent survey of Australian public libraries found that complaints about sexually explicit content outnumbered all others (251 of 322 responding libraries) although grievances about Internet content generally had decreased from 55 per cent in 2002 to 20 per cent in 2011. Only two per cent of complaints were referred to the Australian Communications and Media Authority whereas most complaints were usually dealt with at the time by staff and “Often these were complaints from library users about what they could see on other people’s screens” (ALIA, 2011:20).

Laughton & Rensleigh’s 2007 investigation into on-line pornography at Johannesburg University, based on a questionnaire survey completed by approximately 1000 students on five campuses, found that the majority of respondents had experienced content being blocked at some time of which over half was academic information (52.1 per cent). Eighty per cent of respondents had not been exposed to unsolicited pornography and when asked whether they used the PCs to access pornography, 88.4 per cent stated ‘never’ whilst a small percentage – 2.2 per cent – used the facilities daily to access pornography.

Poulter et al (2009) writing about the FRILLS project (Forensic readiness for Local Libraries in Scotland) funded by the Scottish Library and Information Council in 2007 explored ‘forensic readiness’ (FR) in public libraries - “technical preparedness for computer investigation in anticipation of a crime” (2009:4). The literature review for the project found instances of misuse which typically involved pornography. Two online surveys were also carried out with heads of library services and library staff in Scottish public libraries which looked at the effectiveness of AUPs, experience of misuse, how it had been dealt with, training in detection and misuse reporting. They found that serious incidents of misuse were rare. Staff could lock down machines and some were able to view user screens remotely but wanted more training in this area. It was observed that, “There seemed to be no central monitoring of abuse: thus someone banned in one area could potentially shift activity to another” (2009:5).

Gomez & Gould’s paper (2010) which explored the ‘cool factor’ of public access to ICT, based on the Public Access ICT Landscape Study, 2007-9, conducted by the University of Washington, noted that issues of filtering and misuse emerged in their discussion. There were issues of use that were deemed instrumental e.g. homework, social and economic development purposes versus those which were deemed non-instrumental such as social networking, online games and messaging. This resonates with research with Internet users in Singapore’s public libraries who perceived their Internet activity to be research but on further exploration by the authors was primarily email, games, chat and general web searching (Heok & Luyt, 2010).

Pors’ study of Internet use in public libraries in Denmark found that 33 per cent of PLS had registered some kind of misuse incident or suspicion of an incident: “It is evident from the answers that the librarians see misuse not only as phenomena like the downloading of pornographic, racist and Naziist material, but also changing the configuration of the computers, installation of start-up pictures of a dubious kind and different types of noise problems” (Pors 2001:310). Misuse could also include intellectual property issues such as using peer-to-peer technology to download music illegally (Sturges, 2002).

Filtering software

Much of the professional literature relating to public Internet access in libraries in the USA in particular is focussed on the arguments relating to the pros and cons of technical measures to
manage Internet access, primarily, filtering software. Filtering software, which may also be called content-control software, content filtering software, censorware or web filtering software, has been described by Diaz (1999:147) as that which “seeks to keep a user from finding or viewing certain types of material”. The American Library Association and American Civil Liberties Union have been very vocal in their opposition to filtering (Bertot et al, 2010). As Sturges’ reminds us in his monograph exploring public library Internet access in the UK: “The use of filtering software to block access to Internet content is often talked of as if it were merely a technical matter, but in fact it is almost entirely a question of ethics” (Sturges, 2002:55). The next two sections consider the arguments put forward in favour of and against the use of filtering software.

Arguments in favour of filtering

Protection of minors

The protection of children or minors is the primary justification for the use of filtering software. As The Byron Review, an independent review of the risks children face from the Internet and video games in the UK, noted, much of the concern about content on the Internet is focused on sexual content (2008). Colaric (2003) argues that a failure to filter is doing a disservice to children using the library. The author notes that library staff have worked hard to create a perception of the public library as a safe place for a child that offers accurate information; unfiltered Internet access risks damaging this perception. An argument to counter this has been that the absence of technical measures provides an opportunity for children with the support of library staff to develop their information literacy and searching skills. However, Colaric questioned whether this would actually happen, highlighting a body of research into children’s information literacy skills and noting that children aged nine to 12, “have difficulty constructing effective search strategies” (Colaric, 2003:9) whilst children tend to assume that what they find on the Internet is accurate (Schacter, Chung & Dorr 1998 cited in Colaric, 2003).

Pors (2001) suggests that library assistants are more inclined to favour filtering than librarians because assistants interact with users more often and have more first-hand experience of problems related to Internet access.

“The attraction of filtering public access is that it avoids the necessity for fresh legislation, and anticipates the possible interest of police or security services, by removing access to contentious material before it even reaches anyone’s workstation” (Sturges, 2002:38).

It has elsewhere been argued that filtering software offers a greater degree of control to the end user thereby supposedly balancing the right to freedom of expression with the right not to encounter offensive content (Burt, 1997; Auld, 2003; Cronin, cited in Pierce, 2003); however, this argument could be countered by a lack of any statutory right protecting one from encountering such content. Radom notes in a review of the literature that filters are popular choices because they “are relatively affordable and fairly easy to use. Filters are also widely available in the market and there are many models from which to choose” (Radom, 2007:4). “Furthermore, filters arguably require less staff time and effort to implement or maintain than other measures, such as blacklists or whitelists” (Radom, 2007:5).

Arguments against filtering

The arguments against the use of filtered Internet access are principally related to the technical limitations of the software and the ethical implications of restricting access in this way: “It is an acceptable form of censorship for many organisations, but it is in the raw definition of the word,
censorship” (McMenemy & Burton, 2005:22). Filtering software uses site blocking or keyword blocking or a combination of the two. Arguably, filtering is unreliable and for one librarian is reminiscent of a time when public libraries in the USA kept some reading materials in a locked bookcase - “they recall a time I thought had long since gone by” (Ardito, 2001:14).

Over-blocking and under-blocking sites
Comer’s study of public libraries in Indiana, USA, found that 31 per cent of libraries did not use filters whilst 66 per cent of responding libraries did and between them were using more than 20 different filtering products. Thirty-two per cent reported no problems with them whilst 35 per cent had experienced one or more types of problem. Twenty-two per cent said that users were unable to look at the information they required on the Internet (over-blocking). Twenty-one per cent found that their filters were under-blocking (Comer, 2005).

A report from the Free Expression Policy Project undertaken at Brennan Center for Justice, USA includes a compendium of research which has explored filtering. The report considers the results of research papers and reports in relation to their over and under-blocking rates and the authors concur, “one conclusion is clear from all of the studies: filters continue to block large amounts of valuable information” (Heins et al, 2006:73).

Willard reports on the issue of filtering based in some part on discussions on two email groups with school librarians and related communities. Willard took the stance that all teachers should be able to override filters. She discovered frustrations as staff working with children could not use numerous legitimate teaching tools online (2010).

A study of Australian public libraries found 71 per cent of respondents expressing concerns about filtering and the unreliability of filtering software. Of those respondents operating filtering software, 80 per cent reported that users were unable to access legitimate content or the filter allowed undesirable content (ALIA, 2007). In 2011, 44 per cent of respondents had received complaints in relation to filtering. These were related to over blocking of gaming and social networking sites and email access as well as “restricted access because filters blocked valid, legitimate, inoffensive sites in error; limits on file size downloads, and general objections to the ethos of filtering” (ALIA, 2011:23).

In the UK, the Reading Agency undertook an online survey in 2011 to inform thinking around digital reader development in which all public library authorities (PLAs) in England, Scotland and Wales were invited to participate. Responses were received from 52.6 per cent of PLAs. Tools to manage Internet use were identified as a barrier in the development of a digital reading offer: “Firewalls, filters and other IT restrictions make it hard for staff and users to access social media sites in particular” (Reading Agency, 2011:5). Filters and firewalls were cited by 53.1 per cent and 51.3 per cent respectively of all responding authorities whilst the blocking of social media websites was an obstacle for 46 per cent.

A recent report from the USA commissioned by the ALA and written by a consultant to the ALA’s Office for Information Technology Policy (OITP), explores the impacts of filtering on K-12 education and on public library users’ access to information. The author argues that “Filtered content today, particularly in schools, includes entire social media and social networking sites as well as interactive or collaborative websites – far beyond what the law requires” (2014:1). Drawing on background

---

2 K-12 is a term used in the US, Canada, Australia and elsewhere to denote the entire period of all primary and secondary education.
Managing Access to the Internet 20 REVIEW OF LITERATURE

in Public Libraries

research, presentations and discussion at a national symposium and two online forums in 2013, it is argued that: “Over-filtering affects information access and learning opportunities for both children and adults, and disproportionately impacts those who can benefit from public Internet access the most: the 60 million Americans without access to either a home broadband connection or smartphone” (2014:1). Moreover: “Filtering in libraries causes some patron needs to go unmet. Studies and anecdotes recount numerous examples of blocked online resources ranging from those dealing with war and genocide to safer sex and public health” (2014:1-2).

Process for unblocking/overriding/disabling time-consuming and complicated

Although in the US adults are able to ask staff to unblock sites or disable filters, this process is not always a simple one (Sobel, 2003; Kranich, 2004). As Jaeger et al warn, “Even if patrons are not self-conscious about the material they are seeking, the process of requesting unfiltered Internet access could still limit usage... CIPA has no set procedure for requesting the removal of filters, so the process will vary considerably between libraries” (2006:134). It is probable that many users faced with blocking of content will simply refrain from any further attempt to access the content, even if it would have been useful in meeting their information needs. As the American Civil Liberties Union suggested in 2005, public libraries in Rhode Island had gone beyond that which is federally required to be blocked such as obscenity and child pornography to become a censor rather than a purveyor of information. Their survey responses indicated that few users requested deactivation of filters and it was suggested that this was not because blocking is a problem for users but that they are uncomfortable about asking staff: “Whilst some librarians interpret this as a sign that blocking does not burden patrons, an alternative explanation is much more plausible: adults faced with a pop-up that cites ‘adult content’ or ‘sex’ as the reason for denied access are unlikely to approach a librarian for assistance. They are far more likely to simply abandon the search. We suspect that ‘chilling’[^3] is more prevalent than is acknowledged” (2005:17).

Filters can be bypassed

Filtering does not block all objectionable material and some people know how to bypass filters: “A search on ‘bypass Internet filter’ demonstrates just how easily students can find directions” (Willard, 2010:58). Bitso, Fourie & Bothma’s literature review of Internet censorship in nine countries including the UK notes that there are ways in which individuals may circumvent Internet censorship: “There is evidence that with little effort, users are able to evade filters by accessing blocked websites using overseas Web proxies (i.e. intermediate machines that retrieve Web pages on behalf of users for a number of purposes such as increased efficiency and privacy protection) (Feamster et al., 2002)” (Bitso et al, 2012:12).

Filtering decisions are made by commercial interests not librarians

In 2002, Nancy Willard authored a report which reviewed the relationships with religious organisations of eight filtering companies, whose products were being used in American public schools. The investigation was undertaken using searches on Google with the name of the product, key terms associated with the product (technologies and unique categories) and religious terms and an evaluation of companies appearing on a list of Christian websites. Willard found that three of the filtering companies were also selling their product to conservative religious Internet Service Providers (ISPs) whilst the other five companies had functioned as conservative religious ISPs. Radom’s follow-on article detailing Willard’s research found that “at least 15.9 per cent of Indiana public libraries used filters with connections to conservative religious groups in 2005” (2007:1). Kranich, a former ALA President, argues that staff at filtering software companies cannot possibly review all the

[^3]: ‘Chilling’ is a term in which originated from the U.S.A. and Canada to refer to the inability to exercise rights such as free speech in the face of legal sanction.
publicly available websites yet they are unwilling to disclose the criteria they use for filtering, deeming it commercially sensitive information (2004). Moreover, “Some of these commercially available filtering products actually record users’ actions online, and have been recently discovered to have created a new income stream by disclosing young people’s online searches and chat logs to marketing agencies” (Bertot et al, 2010:170).

It has also been noted that there is a difference between librarians selecting resources and withholding them (Diaz, 1999). Decisions not to add items to stock are traditionally taken in the light of limited acquisition budgets and hence the need to prioritise items. The reverse could be said to be true of Internet filtering whereby blocking access to resources entails additional cost (i.e. that of the software itself). Moreover, “While it has been pointed out that librarians have always selected material for library stock and have therefore acted, to an extent, as a filter, filtering software removes selection decisions from librarians and places it in the hands of non-library trained third parties or computer automation” (Hamilton, 2004:163).

**Ethical implications of filtering**
Aside from the limitations of content-control software, much of the debate surrounding management of the Internet focusses on the ethical implications of filtering for members of a profession who aim to provide information freely and without bias. Certainly, the majority of articles reviewed here were anti-filtering in tone (see for example: Sobel, 2003; Trushina, 2004; Cooke, 2006; Radom, R., 2007; McMenemey, 2009). CILIP’s guide to User Privacy in Libraries (CILIP, 2011) states 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” (2011:12-13), yet acknowledges the appropriateness of discouraging users from viewing illegal sites, “associated with child pornography, race hate or terrorism” or PCs being used “for other types of unlawful or undesirable behaviour – notably hacking, spreading viruses or as an aid to criminal activity” (p.12).

As previously stated, the American Library Association has been a vocal opponent of Internet censorship in public libraries. In its Libraries and the Internet toolkit, the ALA is clear that in spite of the CIPA ruling, it “does not recommend the use in libraries of filtering technology that blocks constitutionally protected information” (p.3) and goes on to advise libraries that do use filtering software, “to set their filters at the least restrictive level in order to minimize the blocking of Constitutionally protected speech” (ALA, 2003:10, their emphasis).

In Australia, the Australian Library and Information Association supported the Australian government’s Protecting Australian Families Online (PAFO) initiative for home use (2006) “but does not recommend the use of Internet filtering technology in public libraries” (ALIA, 2007:4).

Internationally, the IFLA Position on Internet Governance is clear that “Measures which may be necessary to ensure the reliable operation of the Internet, control spam, support intellectual property protection and enable individuals to protect their privacy must not be used to limit the rights expressed in the Universal Declaration of Human Rights, especially those in Article 19” (IFLA, 2005). Article 19 sets out a right to “Seek, receive and impart information and ideas in any media and regardless of frontiers” (United Nations, 1948). This right also underpins the IFLA Code of Ethics for Librarians and other Information Workers, which states unequivocally that “Librarians and other information workers reject the denial and restriction of access to information and ideas most particularly through censorship whether by states, governments, or religious or civil society institutions” (IFLA FAIFE, 2012: Article 1). The Standing Committees of the IFLA Libraries for Children and Young Adults Section and the Reading Section accepted a Statement relating to the Internet and children’s library services at the annual World Library and Information Congress in 2007. They
argued that filtering and censorship do not work and advocated effective education of children, parents, teachers and libraries in Internet use (IFLA, 2009).

**Are there other ways of managing Internet use?**

This section details other methods of managing Internet access in public libraries:

**Acceptable use policy/appropriate use guidelines**

“An acceptable use policy (AUP) is a document that a customer must sign and agree to before they are provided with access to the computer facilities” (McMenemy & Burton, 2005:20). AUPs usually detail activities which are not permitted such as viewing pornography or copying copyright protected materials and “tend to be used by organizations to pass some element of liability onto the customer when accessing Internet services” (McMenemy & Burton, 2005:21). In relation to children accessing the Internet, in the UK, an AUP usually has to be signed by a parent or guardian – in some libraries, the parent has to come to the library to complete the form, in some they do not.

Displaying an AUP prominently in the library is also recommended: “Posting policies is a useful deterrent. In addition to policies that warn patrons not to use the computers for illegal purposes, general library behaviour policies should be enforced, without regard to content viewed” (Minow, 2004:11).

In Denmark, there appears to be a relationship between public libraries who experience some kind of misuse incident and the establishment of ethical guidelines (Pors, 2001). Almost 60 per cent of libraries that had registered an incident had guidelines whilst only one-third of libraries who had not experienced an incident had guidelines. This suggests a reactive approach to the development of AUPs, in direct response to incidences of misuse: “Such guidelines and declarations have the objective of setting realistic expectations for users and they will, hopefully, regulate unwanted types of behaviour. Foremost, they give the libraries the possibility of using sanctions against groups of users that violate the ethical code” (Pors 2001:311).

Privacy screens have also been suggested (Curry, 2000): “Many libraries have found that recessed monitors and well displayed Internet use policies, explaining acceptable and unacceptable Internet behaviour enable patrons to understand and take responsibility for online research and entertainment in public places” (Gottschalk:2006).

Having an AUP in place does not guarantee that misuse will cease. For example, a survey of Indiana’s public libraries with a 33 per cent response rate (144 of 434) discovered that 67 per cent had experienced problems with users not following guidelines (Comer, 2005). Poulter et al found that all the libraries questioned in Scotland as part of the FRILLS project had an AUP but “Many responders thought that AUPs were too easily ignored” and in a minority of libraries, “users got no explanation of the AUP” whilst some thought “the legalese used in AUPs was impenetrable, especially to users for whom English was not their first language” (2009:5). On the other hand, research with staff in Singapore’s public libraries suggests AUPs give staff confidence in managing Internet use: “None of the librarians had problems enforcing these rules as IT policies are in place to prevent the downloading of software, access to instant messaging or chat software, gambling, hacking, pornographic and games sites in the library premises by blocking the URLs of these sites from the server in the library. This means users using the library’s multimedia stations to gain access to the Internet have their boundaries restricted” (Heok & Luyt, 2010:483). But as Kranich highlights, “The vast majority of citizens use the Internet and other library materials responsibly, guided by the local library Internet access policies and codes of conduct that address appropriate use and invoke disciplinary action if rules are violated” (Kranich, 2004:16).
Physical location of PCs
As early as 1997, an article from the USA by an academic librarian considered the tensions inherent when there are “competing interests of computer users who wish to access sexually-explicit materials and those who find them offensive” in the library (Young 1997:49). She suggested one solution was rethinking the location of PCs. Similarly, Still & Kassabian, also writing about public Internet access in academic libraries, suggested positioning of furniture to ensure PCs are on public view to “hinder inappropriate use of library terminals” (1999:20). Visually monitoring what is viewed on a PC was also suggested by Willard who argues in favour of school teachers making a shift from blocking to watching children’s Internet activity: “They must physically supervise and on a random basis, several times during the class session, make a request to see a student’s history file” (Willard, 2010:60).

Controlling length of time on PCs/booking systems
A popular choice of booking systems for public access PCs in the UK has been Netloan which requires the library barcode number and PIN as it interfaces with the library management system data to authenticate the computer user (McMenemy, 2009). This in turn has the potential to act as a deterrent to misuse, with the user knowing that history logs of use can be traced to individual users. In Chisenga’s study in Africa, controls in place included restrictions on the length of time that staff or users were allowed to spend on the Internet (Chisenga, ed., 2004).

Monitoring software/data
As well as visually monitoring Internet use, public library services may also monitor usage through the digital history users leave behind. For example, the Australian Library and Information Association’s Internet Access in Public Libraries Survey discovered amongst approximately 200 responses representative of those providing services in more than 820 locations, 67 per cent of libraries monitored use through visual monitoring by library staff and the collection of system data. Sixty-six per cent of libraries collected data primarily about the sites accessed by all users (247 of 288 libraries) and the largest group of libraries use this data to monitor inappropriate Internet access (159 of 430 libraries) as well as to review filtering issues (28) (ALIA, 2011). Staff may also have the technology to view user screens remotely (Poulter et al, 2009).

User education/training
Willard argues that filtering leads to a false sense of security leading “to a failure to teach students how to prevent and respond to accidental access” (2010:58). User education and training is then one way in which staff can help library users help themselves to navigate the Internet safely and legally (see, for example, Kranich, 2004; Heins et al 2006; Byron, 2008; IFLA, 2009). McMenemy & Burton recommend that AUPs are “backed up with a robust Internet skills approach to ensure customers know just what the Internet does and what is out there for them and their children” (McMenemy & Burton, 2005:21) and note that “The AUP is not a panacea for all problems, but it must be used robustly with confidence and full knowledge of its contents by all staff” (McMenemy & Burton, 2005:22).

Certainly, the literature reveals that public library staff are helping train and support library users with their ICT skills but does not indicate whether this is in relation to accessing Internet content. Jaeger et al (2006), exploring the implications of the Public Libraries and the Internet 2004: Survey Results and Findings funded by the Bill and Melinda Gates Foundation and the American Library Association, found that in the USA ICT training is provided for seniors (57.3 per cent), users with no Internet access at home (52.6 per cent) and adults pursuing continuing education (51.2 per cent). Similarly, in Australia, formal Internet training was offered in 54 per cent of libraries some of which included cybersafety and training for parents: “Training aimed at parents and children was offered in
15% of libraries, taking the form of cybersafety, homework and tutoring, and sessions catering for parents, students and toddlers” (ALIA, 2011:16). Poulter et al observed a “lack of awareness of security issues amongst both library users and librarians” and yet public libraries “would be an ideal venue for imparting information about Internet security” (2009:7).

**Impacts on public library staff**

Frontline library staff may have a particular interest in curbing misuse of public Internet access. In Canada, for example, a public library Internet access crisis arose at Ottawa Public Library. A public Internet access policy had been developed which offered open access with a few filtered PCs (39 of 250). However, some staff were unhappy with this as some users were leaving pornographic images on PCs. The union became involved and the local media described the library as a ‘porn palace’. The resulting policy was for children to have access to filtered Internet services only unless their parents gave approval for unfiltered access: “We introduced a requirement for all parents to personally register their approval of unfiltered Internet access for their children” (Cavanagh, 2004: 356).

Public Internet access has impacted on the role of library staff and services: “Some of the suggested new library roles, such as screen monitors and emergency responders are completely new, while others, such as providing training and assistance, are extensions of libraries’ traditional roles” (Kinney, 2010:130). As the People’s Network was rolled out and public library staff undertook ICT training, research which looked at staff attitudes to ICT found that the majority of those surveyed (964 staff completed the questionnaire) felt generally positive about helping the public use the Internet although one-fifth had mixed feelings and eight per cent were negative (Spacey, 2004). This relative indifference and hostility was frequently related to the time involved in helping the public as well as having to deal with technical concerns. Some staff have not found these new roles or extensions of existing roles to their liking. Poulter et al, writing about the FRILLS project in Scottish public libraries discovered that public library staff “found checking for misuse, and dealing with it, extremely unpleasant” (2009:5).

**Conclusions**

This review of the literature pertaining to public access to the Internet in public libraries nationally and internationally has revealed that Internet use in public libraries is an important facilitator of democracy and equality. However, it is also seen as a potential problem due to potential for misuse. According to much of the research, simplistic technical solutions have disappointed. At present, little is known about the management of public Internet access in the UK but a range of solutions have been adopted in different countries.
RESULTS
We begin by presenting the quantitative data from the survey questionnaire that was distributed to all UK Public Library Services. We then outline the findings from each of the qualitative case studies that were carried out.

Survey
Survey data were cleaned and analysed in SPSS v.19 and are reported in the following section. A total of 80 responses was received from a potential 206 services which represents a response rate of 39 per cent. In terms of country, 75.0 per cent of respondents are from English public library services, 15.0 per cent of responses are from Scottish authorities, 8.8 per cent of responses are from Welsh public library services and 1.3 per cent is from Northern Ireland (which represents the single Public Library Authority operating within the region) (Figure 2).

![Figure 2 Geographical response by country](image)

Almost half of respondents defined themselves as senior library management (48.8 per cent) whilst similar proportions were middle management (23.8 per cent) and library IT staff (22.5 per cent) respectively (Figure 3).

![Figure 3 Job category of respondents](image)
Internet access in your libraries

Respondents were asked what library members and non-members (guests) needed in order to access the Internet in their libraries (Figure 4). Almost all services require library members to have a library borrower number (98.8 per cent). In 70 services, a PIN or password is required (87.5 per cent). Seventy respondents (87.5 per cent) indicate 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 per cent).

For guests or non-members, half of responding services require some proof of identity (50.0 per cent) whilst a PIN or password is required by almost half of responding services (47.1 per cent). A quarter of responding services require a means of payment (25.0 per cent). In five services, no authentication is required (7.4 per cent) (Figure 4).

Of those services responding ‘other’ in relation to library members and guests (nine in total), five have some form of temporary ticket or log in for guests: “Guests are logged in via a staff member using a guest ‘ticket’”. In two services, name and address details are required but not proof 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.

![Figure 4 Requirements for Internet access on a library PC](image)

**Figure 4** Requirements for Internet access on a library PC

Booking system

Over 90 per cent of responding services use a proprietary software booking system (92.4 per cent) (Figure 5). Three services do not have a booking system. Over half of those using a proprietary booking system use Netloan by Lorensbergs (54.8 per cent) whilst almost one third use i-CAM by Insight Media Internet Limited (Figure 5).
The Internet is free to use in 50 responding public library services (63.3 per cent) (Figure 6). In 20.3 per cent of services, there is a charge for visitors/non-members. A minority of responding services operate a charging system for Internet users with some element of free use followed by a fee (16 services in total). In one service, all Internet users have to pay.

Eleven respondents detailed the situation in their service with regard to Internet access, having responded ‘other’. In five services, library members are permitted between 45 minutes and 2 hours free Internet access and then charges are applicable: “Library Members with Local Discount Card (Advantage Card) have 45 minutes free and then pay for additional time”. In three services, there are different rates for concessions: “Everyone pays apart from concessions - unemployed, children under 19, students, older adults, disabled”. In one service, Internet use is free if the individual has a membership card from any UK public library authority. One service operates a subscription service for Internet use: “We have a yearly subscription for library members. Guest users pay by the hour. Job seekers get free subscription for 3 months”.
WiFi

More than four fifths (83.8%) of responding library services offer WiFi access to the public at one or more of their libraries (n=67). To access WiFi, a PIN or password is the most common requirement of library members (61.2 per cent) and of guests (39.6 per cent) (Figure 7). Almost half of responding services require library members have their borrower number (49.3 per cent) although in almost one-fifth of responding services, no authentication is required for library members (19.4 per cent). For guests, proof of identity (28.3 per cent) and no authentication required (26.4 per cent) are also regular options. Of those selecting ‘other’, analysis of comments submitted reveals that requirements include e-mail address (5), a mobile telephone number (2), use of a guest card/log-in (2), accepting the AUP or Internet use policy (2), setting up an account (1) or adhering to the WiFi supplier’s terms and conditions (4).

![Figure 7 Requirements of users in order to access WiFi](image-url)
Overwhelmingly, of the 67 responding services that provide WiFi, the majority provide filtered access to the Internet (83.6 per cent) (Figure 8).

![Pie chart showing filtered access to the Internet](image)

**Figure 8** Is WiFi access filtered?

Over half of responding services provide secure WiFi access – WPA or WPA2 (59.7 per cent), however, approximately one quarter of respondents do not provide secure access (25.4 per cent) and 10 services did not know (14.9 per cent) (Figure 9).

![Pie chart showing secure WiFi access](image)

**Figure 9** Is WiFi access secure?
Approximately four-fifths of public library service WiFi users see a special web page known as a captive portal to log-on/authenticate before using the Internet (80.6 per cent) (Figure 10).

**Filtering**

All 80 responding UK public library services provide filtered access to the Internet on all their PCs (100.0 per cent). The decision to install filtering software (Figure 11) appears to be have been led by the IT departments of local authorities (26.3 per cent), by library service senior management (25.0 per cent) and by local authority senior management (22.5 per cent).
Two-fifths of respondents use WebSense filtering software (40.0 per cent). Bluecoat was the second most popular filtering package used (11.3 per cent) (Table 2).

<table>
<thead>
<tr>
<th>Filtering software package used</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>Netsweeper</td>
<td>3</td>
<td>3.8</td>
</tr>
<tr>
<td>Smoothwall</td>
<td>3</td>
<td>3.8</td>
</tr>
<tr>
<td>Sophos</td>
<td>3</td>
<td>3.8</td>
</tr>
<tr>
<td>Bloxx</td>
<td>2</td>
<td>2.5</td>
</tr>
<tr>
<td>FortiGate</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>McAfee</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>SurfControl</td>
<td>2</td>
<td>2.5</td>
</tr>
<tr>
<td>Atomwide</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Barracuda</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Cisco</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>CLEO OneConnect</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Dell SonicWALL</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>E2BN Protex</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>RM SafetyNet Plus</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>SmartFilter</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>Don't know</td>
<td>4</td>
<td>5.0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>80</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Table 2 Filtering software package used
Blocking

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

The top five content categories blocked for all users are sexual (85.7 per cent), hacking (83.1 per cent), violence and intolerance/hate (both 80.5 per cent) and extremist (79.2 per cent). The least blocked content for all users are finance/banking (0 per cent), social networking (1.3 per cent), collaborative sites such as wikis (1.3 per cent), blogs (3.9 per cent) and personals/dating (5.2 per cent) (Table 3).

Amongst respondents selecting ‘only for children’, the top five content categories blocked are personals/dating (53.8 per cent), social networking (51.3 per cent), gambling (46.2 per cent), chat (33.3 per cent), weapons and bad language (both 28.2 per cent). The least blocked content ‘only for children’ are RSS feed aggregators and file download/upload (both 5.1 per cent), television (7.7 per cent), collaborative sites (7.7 per cent) and hacking and blogs (all 10.3 per cent).

The top five content categories blocked ‘only for teenagers’ are gambling and personals/dating (both 45.8 per cent), weapons (29.2 per cent), bad language (25.0 per cent) and illegal drugs (20.8 per cent) and the least blocked are instant messaging, RSS feed aggregators, file download/upload and webmail (all 0 per cent).

Analysis of the comments provided for ‘other’ 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 included school cheating information, historical revisionism and residential IP addresses.
<table>
<thead>
<tr>
<th>Category</th>
<th>All users (Frequency)</th>
<th>Frequency</th>
<th>Per cent</th>
<th>Only for children (Frequency)</th>
<th>Frequency</th>
<th>Per cent</th>
<th>Only for teenagers (Frequency)</th>
<th>Frequency</th>
<th>Per cent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sexual</td>
<td>66</td>
<td>85.7</td>
<td></td>
<td>6</td>
<td>15.4</td>
<td></td>
<td>3</td>
<td>12.5</td>
<td></td>
</tr>
<tr>
<td>Hacking</td>
<td>64</td>
<td>83.1</td>
<td></td>
<td>4</td>
<td>10.3</td>
<td></td>
<td>2</td>
<td>8.3</td>
<td></td>
</tr>
<tr>
<td>Violence</td>
<td>62</td>
<td>80.5</td>
<td></td>
<td>5</td>
<td>12.8</td>
<td></td>
<td>3</td>
<td>12.5</td>
<td></td>
</tr>
<tr>
<td>Intolerance/Hate</td>
<td>62</td>
<td>80.5</td>
<td></td>
<td>6</td>
<td>15.4</td>
<td></td>
<td>3</td>
<td>12.5</td>
<td></td>
</tr>
<tr>
<td>Extremist</td>
<td>61</td>
<td>79.2</td>
<td></td>
<td>6</td>
<td>15.4</td>
<td></td>
<td>4</td>
<td>16.7</td>
<td></td>
</tr>
<tr>
<td>Spyware</td>
<td>58</td>
<td>75.3</td>
<td></td>
<td>6</td>
<td>15.4</td>
<td></td>
<td>2</td>
<td>8.3</td>
<td></td>
</tr>
<tr>
<td>Proxy avoidance</td>
<td>54</td>
<td>70.1</td>
<td></td>
<td>6</td>
<td>15.4</td>
<td></td>
<td>2</td>
<td>8.3</td>
<td></td>
</tr>
<tr>
<td>File sharing/peer-to-peer</td>
<td>52</td>
<td>67.5</td>
<td></td>
<td>5</td>
<td>12.8</td>
<td></td>
<td>1</td>
<td>4.2</td>
<td></td>
</tr>
<tr>
<td>Illegal drugs</td>
<td>49</td>
<td>63.6</td>
<td></td>
<td>8</td>
<td>20.5</td>
<td></td>
<td>5</td>
<td>20.8</td>
<td></td>
</tr>
<tr>
<td>Criminal skills</td>
<td>46</td>
<td>59.7</td>
<td></td>
<td>6</td>
<td>15.4</td>
<td></td>
<td>3</td>
<td>12.5</td>
<td></td>
</tr>
<tr>
<td>Weapons</td>
<td>45</td>
<td>58.4</td>
<td></td>
<td>11</td>
<td>28.2</td>
<td></td>
<td>7</td>
<td>29.2</td>
<td></td>
</tr>
<tr>
<td>Gambling</td>
<td>34</td>
<td>44.2</td>
<td></td>
<td>18</td>
<td>46.2</td>
<td></td>
<td>11</td>
<td>45.8</td>
<td></td>
</tr>
<tr>
<td>Bad language</td>
<td>25</td>
<td>32.5</td>
<td></td>
<td>11</td>
<td>28.2</td>
<td></td>
<td>6</td>
<td>25.0</td>
<td></td>
</tr>
<tr>
<td>Instant messaging</td>
<td>23</td>
<td>29.9</td>
<td></td>
<td>9</td>
<td>23.1</td>
<td></td>
<td>0</td>
<td>0.0</td>
<td></td>
</tr>
<tr>
<td>Chat</td>
<td>14</td>
<td>18.2</td>
<td></td>
<td>13</td>
<td>33.3</td>
<td></td>
<td>4</td>
<td>16.7</td>
<td></td>
</tr>
<tr>
<td>File download/upload</td>
<td>12</td>
<td>15.6</td>
<td></td>
<td>2</td>
<td>5.1</td>
<td></td>
<td>0</td>
<td>0.0</td>
<td></td>
</tr>
<tr>
<td>Online gaming</td>
<td>11</td>
<td>14.3</td>
<td></td>
<td>8</td>
<td>20.5</td>
<td></td>
<td>4</td>
<td>16.7</td>
<td></td>
</tr>
<tr>
<td>RSS feed aggregators</td>
<td>9</td>
<td>11.7</td>
<td></td>
<td>2</td>
<td>5.1</td>
<td></td>
<td>0</td>
<td>0.0</td>
<td></td>
</tr>
<tr>
<td>Television e.g. 4OD, i-Player</td>
<td>7</td>
<td>9.1</td>
<td></td>
<td>3</td>
<td>7.7</td>
<td></td>
<td>2</td>
<td>8.3</td>
<td></td>
</tr>
<tr>
<td>Personals/dating</td>
<td>4</td>
<td>5.2</td>
<td></td>
<td>21</td>
<td>53.8</td>
<td></td>
<td>11</td>
<td>45.8</td>
<td></td>
</tr>
<tr>
<td>Blogs</td>
<td>3</td>
<td>3.9</td>
<td></td>
<td>4</td>
<td>10.3</td>
<td></td>
<td>2</td>
<td>8.3</td>
<td></td>
</tr>
<tr>
<td>Webmail</td>
<td>2</td>
<td>2.6</td>
<td></td>
<td>7</td>
<td>17.9</td>
<td></td>
<td>0</td>
<td>0.0</td>
<td></td>
</tr>
<tr>
<td>Collaborative sites e.g. wikis</td>
<td>1</td>
<td>1.3</td>
<td></td>
<td>3</td>
<td>7.7</td>
<td></td>
<td>1</td>
<td>4.2</td>
<td></td>
</tr>
<tr>
<td>Social networking e.g. Facebook, Twitter</td>
<td>1</td>
<td>1.3</td>
<td></td>
<td>20</td>
<td>51.3</td>
<td></td>
<td>4</td>
<td>16.7</td>
<td></td>
</tr>
<tr>
<td>Finance/banking</td>
<td>0</td>
<td>0.0</td>
<td></td>
<td>7</td>
<td>17.9</td>
<td></td>
<td>4</td>
<td>16.7</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>17</td>
<td>22.1</td>
<td></td>
<td>4</td>
<td>10.3</td>
<td></td>
<td>4</td>
<td>16.7</td>
<td></td>
</tr>
<tr>
<td><strong>Number of respondents</strong></td>
<td><strong>77</strong></td>
<td><strong>100.0</strong></td>
<td></td>
<td><strong>39</strong></td>
<td><strong>100.0</strong></td>
<td></td>
<td><strong>24</strong></td>
<td><strong>100.0</strong></td>
<td></td>
</tr>
</tbody>
</table>

Table 3 Categories of sites blocked for all users, only for children and only for teenagers

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 per cent) (Figure 12). In half of responding services Internet users can email a request to the library service. Approximately one fifth of services give users the opportunity to complete a request form online (21.3 per cent) or complete a paper form in the library (22.5 per cent). 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.

Responsibility for responding to requests to change the filter belongs to library service senior management in over half of responding services (52.5 per cent) and by IT staff at local authority level (41.3 per cent) and library service level in approximately two-fifths of services (41.3 per cent) (Figure 13). Fifty three respondents selected only one option (66.3 per cent) whilst 27 respondents (33.8 per cent) selected more than one option. Fourteen respondents selected two options (17.5 per cent) and 10 respondents selected three options (12.5 per cent).

Figure 12 How to Request a change in the filtering policy

Figure 13 Responsibility for responding to filter change requests

Fewer than 10 per cent of library services give frontline library staff the responsibility to respond to filtering requests. Six respondents selected ‘other’. Their comments reveal that most of those staff have ICT responsibility including information security or virtual content. One respondent did not know about the process in their service as their filtering policy is under development. In one service, the IT service is outsourced to Capita and filtering responsibility rests with them.
In the majority of public library services, library users are made aware that the library employs filtering software in the Acceptable Use Policy (88.8 per cent) (Figure 14). Over half of responding services draw users’ attention to the use of filtering software when they log-on to the PC (56.3 per cent). Over half of responding services inform the public on the library website that Internet content is filtered (51.3 per cent). Of respondents selecting ‘other’ (6), three services did not specifically make users aware of Internet filtering: “We don’t advertise that we use filtering software”. In two services, users were notified electronically either by a message on the computer screen or at the point of filtering whilst A5 paper hand-outs were used in one service.

![Figure 14 Ways in which library users are made aware of Internet filtering](image)

**Complaints**

Respondents were asked if 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 (65.8 per cent) compared to 30.4 per cent who had not. A very small proportion of respondents did not know (3.8 per cent) (Figure 15).

![Figure 15 Complaints about the Internet filter](image)
Of those services that had received complaints (52), over-blocking was the most frequent cause (88.5 per cent) whilst the technical limitations of access such as the inability to upload or share files was also cited by over half of respondents receiving complaints (53.8 per cent) (Figure 16). Less numerous were complaints about the use of filtering software per se (19.2 per cent). ‘Other’ complaints include users being unable to access online greetings cards, a drug related website and access to virtual learning environments (VLEs).

<table>
<thead>
<tr>
<th>Type of complaint</th>
<th>No. of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over-blocking i.e. user unable to access legitimately required content</td>
<td>46</td>
</tr>
<tr>
<td>Technical limitations of access (e.g. inability to download/upload/file share)</td>
<td>28</td>
</tr>
<tr>
<td>Objection to use of filtering software</td>
<td>10</td>
</tr>
<tr>
<td>Other</td>
<td>6</td>
</tr>
</tbody>
</table>

**Figure 16** Types of complaint about Internet filtering

Respondents were asked their opinion of filtering. How useful did they judge it in maintaining acceptable Internet use in their libraries? Over half of respondents judge it to be ‘very useful’ (56.3 per cent) and approximately two-fifths find it ‘somewhat useful’ (41.3 per cent). Only two respondents were negative about filtering, judging it to be ‘not very useful’ (2.5 per cent) (Figure 17).

Approximately two-fifths of respondents thought that library users sometimes circumvented the Internet filter (41.3 per cent). However, around a third perceived that it rarely happened (33.8 per cent). Around one fifth of respondents did not know (21.3 per cent) (Figure 18). None thought it was a frequent problem.

**Figure 17** Opinions of the usefulness of filtering
Acceptable Use Policies

All but one of the responding services reported having an Acceptable Use Policy for the Internet (98.8 per cent), whilst one respondent did not know whether one existed.

In terms of the formulation of the AUP, senior library service management was usually involved (87.3 per cent), while in over half of responding services, library service IT staff were involved (55.7 per cent) (Figure 19). In just under half of responding services, the local authority’s legal staff and IT team were involved (45.6 and 45.6 per cent respectively). Councillors were involved in its formulation in fewer than 10 per cent of services. ‘Other’ colleagues involved included Information Security staff and in one authority a combination of library service IT, senior management and corporate IT.

![Figure 18 Perception of the frequency of filter circumvention by users](image1)

![Figure 19 Staff involved in the formulation of service’s AUP](image2)
In around half of services the AUP was signed off at senior library service management level (50.6 per cent). Fewer services had their AUP signed off by the legal department of their local authority (13.9 per cent), by local authority senior management (11.4 per cent) or by elected members (10.1 per cent) (Figure 20).

![Figure 20 Staff involved in signing-off the AUP](image)

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 (89.9 per cent) whilst in just under half of responding services, there is information on the library website (48.1 per cent). The AUP is also highlighted on the PC/Internet use form (34.2 per cent), the library membership form/pack (27.8 per cent) and posters in the library (22.8 per cent) (Figure 21). ‘Other’ ways include hand-outs in the library (two services) and staff, presumably making users aware of its existence.
Major breaches of the AUP are known to occur ‘rarely’ (38.0 per cent) or ‘sometimes’ (31.6 per cent) in the majority of responding authorities. According to 10 respondents, breaches ‘never’ happen (12.7 per cent) whilst in 14 services, the respondent did not know (17.7 per cent) (Figure 22).

Overwhelmingly, breaches are a result of library users viewing obscene (legal and illegal) content (80.0 per cent) (Table 4). Viewing racist, extremist or hate content was noted in five services (11.1 per cent). Fewer than 10 per cent of responding services’ AUP breaches involved viewing violent content, online bullying/harassment and hacking (each 8.9 per cent), malware/viruses (6.7 per cent) or copyright infringement (4.4 per cent). ‘Other’ breaches include criminal activity (four) including “Viewing inappropriate content in relation to bail orders and sending hate mail” and “Bomb making, reported to Police and led to prosecution”. Damage to equipment, users attempting to log-in with other users’ details and inappropriate user behaviour were also mentioned.

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Per cent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing of obscene (legal and illegal) content</td>
<td>36</td>
<td>80.0</td>
</tr>
<tr>
<td>Viewing of racist, extremist or hate content</td>
<td>5</td>
<td>11.1</td>
</tr>
<tr>
<td>Online bullying/harassment</td>
<td>4</td>
<td>8.9</td>
</tr>
<tr>
<td>Viewing of violent content</td>
<td>4</td>
<td>8.9</td>
</tr>
<tr>
<td>Hacking</td>
<td>4</td>
<td>8.9</td>
</tr>
<tr>
<td>Malware/viruses</td>
<td>3</td>
<td>6.7</td>
</tr>
<tr>
<td>Copyright infringement</td>
<td>2</td>
<td>4.4</td>
</tr>
<tr>
<td>Spaming</td>
<td>1</td>
<td>1.8</td>
</tr>
<tr>
<td>Other breaches</td>
<td>8</td>
<td>17.8</td>
</tr>
<tr>
<td><strong>Number of respondents</strong></td>
<td><strong>45</strong></td>
<td></td>
</tr>
</tbody>
</table>

Table 4 Types of major AUP breaches
Minor breaches appear to happen more frequently than major breaches, occurring ‘a lot’ in 3.8 per cent of responding services and ‘sometimes’ in 39.2 per cent of responding services (Figure 23). However, the largest proportion of respondents felt that minor breaches rarely happened (43.0 per cent).

Figure 23 Minor breaches of the AUP

Overwhelmingly, minor breaches of the AUP involve users viewing obscene content (92.7 per cent) (Table 5). ‘Other’ breaches include attempts to change PC settings and the PC booking system, viewing unacceptable materials, streaming TV, using other people’s log-in details and unacceptable behaviour.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Per cent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing of obscene (legal and illegal) content</td>
<td>51</td>
</tr>
<tr>
<td>Viewing of violent content</td>
<td>9</td>
</tr>
<tr>
<td>Online bullying/harassment</td>
<td>6</td>
</tr>
<tr>
<td>Malware/viruses</td>
<td>6</td>
</tr>
<tr>
<td>Viewing of racist, extremist or hate content</td>
<td>6</td>
</tr>
<tr>
<td>Copyright infringement</td>
<td>6</td>
</tr>
<tr>
<td>Hacking</td>
<td>2</td>
</tr>
<tr>
<td>Spamming</td>
<td>1</td>
</tr>
<tr>
<td>Other breaches</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 5 Types of minor AUP breaches

Additional measures
The most commonly used additional measure to manage public Internet access is visual monitoring by library staff (83.5 per cent). The positioning of PCs and use of a booking system are also popular mechanisms (70.9 per cent). Collecting Internet use data is utilised by over two-fifths of respondents (44.3 per cent) whilst monitoring software is used in almost a third of responding services (30.4 per cent) (Figure 24).
‘Other’ additional measures include staff being vigilant, rather than systematic visual monitoring of 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, ‘computer buddies’, take place in one service. Two services utilise technological measures such as adjusting the filtering categories whilst in one service, monitoring software is about to be introduced.

**Staff training**

Less than one-fifth of respondents indicated that public library staff receive regular Internet training (17.5 per cent) *(Figure 25).*
Minors
Overwhelmingly, all terminals have filtering software to protect minors (96.3 per cent) (Figure 26). In over half of responding services, minors access the Internet in a dedicated area with oversight by staff (53.8 per cent). Almost half of services rely on parental oversight of use (48.8 per cent) and adherence to the AUP in addition to the filtering software (47.5 per cent). In one quarter of services, minors have dedicated terminals, which are usually located in a dedicated area (25.0 per cent). User education tailored to minors is used in 11 authorities (13.8 per cent).

![Figure 26 Measures to protect minors using the Internet](image)

Misuse incidents involving minors happen rarely according to approximately two-fifths of respondents (43.8 per cent). Thirty per cent of respondents reported that they never happen whilst in 12.5 per cent of responding services, they sometimes happen. Eleven respondents (13.8 per cent) did not know (Figure 27).

![Figure 27 Frequency of incidents involving minors and misuse](image)

Respondents were asked to state what they feel works particularly well with regard to managing public access to the Internet in their services. Responding to this question was optional. The
comments submitted were analysed thematically and the results are presented in Table 6. Use of filtering software and an electronic booking system for Internet use are both popular options to manage Internet access:

“WebSense filtering and i-CAM PC booking system”.

“Having filtering software (we changed to Finjan about 2 years ago). The previous filtering software was not as robust and we had particular issues with hacking and access to terrorist web sites”.

“A robust filter and booking software”.

<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>WiFi</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</td>
</tr>
</tbody>
</table>

Table 6 Respondents’ views of what works well in relation to managing public Internet access
Case Studies

Case study 1: Derbyshire

Researchers visited Derbyshire’s principal library, Chesterfield, where they interviewed six members of staff at different organisational levels within Cultural and Community Services, the department which includes library services: an Assistant Director, Service Relationship Manager, Senior Librarian, Access and Inclusion Librarian, Assistant Library Manager and Library Assistant. In addition, members of the public using the library PCs were approached and asked to participate in interviews. Four members of the public volunteered and were interviewed in situ. In addition to the online survey response completed by a senior member of the library service, a search of relevant documentation highlighted a number of local authority policy papers, commercial web pages and other related literature which was also reviewed.

Context

Derbyshire is an English county in the East Midlands and whilst its administrative headquarters is based in Matlock, Chesterfield is its largest town with its busiest library. Indeed, Chesterfield Library was the seventh busiest library in the UK in terms of issues per annum and the busiest in the East Midlands (2011-2012) (CIPFA 2012). Derbyshire has 45 static libraries and ten mobile libraries.

Derbyshire County Council was one of the first public library authorities to provide Internet access to the public prior to the rollout of the People’s Network. In 1997, the authority’s Libraries and Heritage Department secured a bid from the Public Libraries Challenge Fund (which was a partnership between the Department for Culture, Media and Sport and the Wolfson Foundation) to install a network of 30 computers in 11 of its largest libraries. In early 1998 the network was installed and Derbyshire Learning and Technology Access (DELTA) was launched. Derbyshire also secured funding in the second year of the Wolfson Fund4 for installing computers in some of its smaller libraries and in 1999/2000 won a third award which meant that Internet access would be rolled out to three large mobile libraries.

Library users in Derbyshire now have access to over 400 static desktop PCs which are installed with Windows 7 and Office 2010. They provide free access to the Internet and in 2011-2012, offered a potential 542,546 hours of which 233,389 were recorded as used (43.0 per cent) (CIPFA 2012). The PCs can be booked up to six days in advance and for up to one hour at a time. Wireless Internet access (WiFi) is available in 20 of the county’s 45 static libraries. It was rolled out in the first ten in 2008. This is also free to use.

ICT support for the public includes, for example, sessions in genealogy with staff in the Local Studies department of Chesterfield Library. More intensive support is provided by staff and volunteers – previously known as computer buddies, now called ICT volunteers. This scheme emerged from development work carried out as part of Best Value5 involving local over 50s groups. There are approximately 20 ICT volunteers who assist the public in any of the seven Learning and Training suites across the county. At Chesterfield Library a team of 4-5 volunteers is managed by one of the Community Learning and Information team.

---

4 The DCMS/ Wolfson Programme awarded funding for projects intended to enhance the role of public libraries in promoting reading as a skill and a pleasure.
5 Best Value was introduced in England and Wales as part of the Local Government Act 1999 and came into force in 2000, with the aim of improving the provision of local public services both in terms of cost and of quality. In Wales it is known as the Wales Programme for Improvement.
Managing Internet access

In order to access the Internet on stand-alone PCs, members of the library need their library borrower number and PIN or password. No user identification is required to access the free WiFi network. Children under the age of 12 must be joined by a parent or guardian who must bring some form of identification with their own name and address, whilst children over the age of 12 may join if they have some identification with them which shows their name and address. Non-members or guests need to produce proof of identity to staff.

Derbyshire Libraries provide filtered access to the Internet for the public on both the cable networked PCs and the WiFi connection. However, filtering of access is not advertised to users. Users questioned included those who were aware filtering was in place based on their experiences when using the Internet and those who did not:

“And going on YouTube, I wanted to watch Saddam Hussein get hung but it wouldn’t let me”.

“No, I didn’t think it was... I didn’t think it was because of some of [the sites] people can get on”.

“I’m aware that they must do something like that because there’s a clause that you always agree to go on that, it more or less says that you agree to abide by their policies and procedures and I’d be very surprised if a library didn’t filter the Internet”.

“Not off hand but I wouldn’t try it out to find out”.

Filtering is perceived by staff as helping to provide a safe environment, reassuring parents whose children wish to access the Internet in the library and helping to prevent illegal use:

“Obviously there is material available on the Internet it is illegal to possess or download and also there is material that would be unsuitable for children or younger people to access and so I think we have a duty of care to ensure that, for instance, children’s requirements for a safe environment are catered for”.

Reflections on Internet provision prior to filtering were that it was more problematic because the same small number of library users were repeatedly misusing the service: “In the days before we had filtering software, I think we had some occasions where people did access things that they shouldn’t be accessing and it seemed to be a constant battle to talk to people and we had several people who we had seen on a number of occasions and they’d say ‘Oh no, it won’t happen again etc.’ and it does”.

In spite of some early philosophical reservations about filtering, in practical terms, staff agreed with the decision: “So I suppose, pragmatically, I’ve realised that although I may have had ethical concerns as a librarian, the reality is, I suspect, that for the half a million uses we have every year, I’m not under the impression that it’s caused any particular problems”.

Staff were of the opinion the filtering software had improved over the years such that in recent times staff had not received any complaints about the filter blocking legitimate sites. The number of Internet users who attempt to access something on the Internet that is blocked and do not alert staff is unknown.

No real disadvantages were identified in having filtering in place.
A council decision was made to switch to Fujitsu as the library Internet Service Provider who employ filtering software from Websense®. However, Internet filtering had been in place prior to this contract.

Derbyshire Libraries have an Acceptable Use Policy (AUP) which is looked at regularly. The AUP appears on PC screens at the start of a public session. It is a short, concise statement which asks users to agree that they will not create, access, copy, store, transmit or publish any material which is obscene, racist, defamatory, illegal; causes harassment or gross offence or would breach copyright. If users do not accept or abide by the AUP their access to the Internet will be withdrawn. Internet users are also informed that their use may be monitored but not how this will be undertaken. They must use their own library card and may not watch live TV broadcasts.

Derbyshire County Council has recently acquired new Internet booking software – Netloan, from Lorensbergs. A tender process for a self-service booking system began in 2009 to which 14 suppliers responded. In early 2011, the Strategic Director, Cultural and Community Services recommended to the Cabinet Member for Leadership and Culture the procurement of Netloan. It was estimated that the saving in staff time would equate to 1.5 FTE. Prior to this, Library Assistants would look after the computer bookings. However, whilst staff time has been reduced in relation to bookings, staff time is required in releasing prints to Netloan although this is under review.

Library staff liaise with Transformation Services (TS) (located within Corporate Resources and Human Resources) which is a centralised ICT team. The Service Relationship Manager is responsible for the libraries’ ICT systems and infrastructure and works in conjunction with TS. Staff have a telephone number they can call initially if a problem arises. At Chesterfield there is also a technician within the library who can help with some hardware issues as opposed to software problems. Library users may request a site is unblocked by asking staff or emailing the library service although there does not appear to be a direct link on the website to request a change to the library filter.

Ethical considerations
Staff are aware that there are ethical issues around controlling content but all were happy with the use of filtering for a number of reasons including its practicality. There are simply not enough staff or staff with the capacity to monitor what library users are looking at on the PCs: “Given how staffing is in the library, people would probably agree, there’s less chance to say ‘Well, I’m just going to check that they are not file-sharing or downloading illegal music or watching live television or something’. So I don’t think we are monitoring that greatly. I think we are probably relying on things like the software to do the business about unsuitable sites”. Creating an environment that is welcoming to families with children was another strong motivation. Issues of legality were also noted.

Managing misuse
There have been no major incidents of misuse or evidence of misuse and relatively few complaints about the filtering software in recent times. In the past, staff did experience users complaining that legitimate sites were being blocked which were classed as ‘alternative’ by the software: “When we first had this system we had things like people couldn’t get onto sites for vegetarians”.

Within the last five years, a member of the public complained about the filtering software blocking access to a political site, the British National Party, for which they were the local candidate. As the website is legally available, communications with the ISP and colleagues within Transformation Services resulted in the site being unblocked. Incidents such as these tend to reach the ears of the second tier of management within Derbyshire Libraries i.e. Assistant Director level, but less controversial issues are unlikely to escalate that high and would probably be dealt with at level three (Service Delivery Manager).
There is a range of sanctions in use for incidents of misuse. Staff can speak to individuals and end their Internet session immediately, however, if they don’t feel comfortable doing that they may refer the issue to their duty manager or in the case of Chesterfield Library to a member of security. There are a series of bans from accessing the Internet which could be for three, six or nine months which would be communicated to a library user in a letter.

Library users’ Internet histories can be accessed. However, this is not something that staff in the library service are able to do and requires the assistance of a colleague in Transformation Services. The AUP states that “Your Internet use may be monitored and action taken if you breach this Acceptable Use Agreement”; however, it does not state how long the log is kept by DCC. The log of a particular machine would only be investigated if another user complained that someone had viewed pornography or terrorist material, for example, or if the police requested such information: “I think there are one or two people in our Transformation team who are equipped and able to do that...If you said to me ‘Who’s been on PC14 upstairs today?’ we’d have to go through a process to get somebody to look at that machine but it can be done”.

Misuse is perceived as a minor problem of which accessing pornography is the most prevalent: “Apart from young boys looking at naked women and then you say ‘That’s not suitable’ and then they stop. I haven’t had anything beyond that myself”.

In relation to online copyright, management assume that professional librarians in the service are cascading and sharing good practice with other staff across the service. There are occasional staff briefings on copyright. Informally, one member of staff has become something of a copyright expert to whom other staff refer. Library users are reminded about copyright in the AUP and there are posters about copyright generally, displayed in all libraries.

Internet users are not permitted to install their own software on the library PCs. File sharing is not permitted. In terms of the implications of the Digital Economy Act on the service, management feel that it is not clear that the DEA is applicable to libraries.

Staff
Staff switch the PCs and the printer on in the morning and off again at the end of the day. They assist users with logging on to the PCs, printing and making Internet bookings. All front-line library staff assist users with the Internet but staff ICT skills are as varied as those of library users. This can present a challenge for staff as can the constraints of time: “The rest of it is really what you pick up as you go along and I think a lot of us are self-taught really and I think you’re sometimes embarrassed that the customer knows more than you do, I mean, there are some real experts out there”. Library users requiring more intense support than front-line staff can provide are encouraged to book on to Internet taster sessions where they receive one-to-one assistance. A lot of staff completed the European Computer Driving Licence (ECDL) as part of the People’s Network ICT training initiative in the early 2000s. There is no regular Internet training for staff but they are able to attend in-service courses and are supported by their peers. However, not all staff have Internet access at home such is the nature of broadband penetration in Derbyshire. Frontline staff felt that new and refresher ICT training is overdue and suggestions included online training.

Staff also have training on how to deal with difficult customers and customers with mental health issues which can come in useful in relation to managing Internet use.

Issues
Offensiveness is subjective. Upon further investigation what may be seen as misuse is one person’s perception of what is offensive compared to another’s. While perceptions of appropriateness are not
the same as what is legal, one member of staff inferred legality is more important but on a day to
day basis staff have to make decisions about appropriateness as this example illustrates:

“You see it’s about perception of what is acceptable or not and some people perceived that this
person was misusing the Internet and looking at images that they felt to be unsuitable. But that was
further investigated, you know, I spoke to a senior colleague about it and she spoke with this person
and the decision was made that the sites they were looking at were women’s wrestling websites but
someone had perceived the images not to be suitable. So it’s really deciding... giving people
freedom to look at sites”.

Future
Staff perceive that the service still has a role to play in providing Internet access. It was noted that in
the East Midlands, Derbyshire has the lowest broadband penetration.

It is anticipated that the numbers of people using portable devices and accessing the library WiFi
connections will increase. However, these data are not currently captured.

Good practice
“It’s a combination of filtering, AUP and staff oversight of PCs. Combined they create an expectation
of reasonable use” (survey comment).

Users

User 1
Unemployed male, 20-34. Accesses the Internet every day at Chesterfield Library as he is on daily
sign in with the Job Centre and does not have any other means of Internet access. He was aware
that the Internet was filtered as he has found some sites blocked but agrees that it should be filtered
particularly in relation to blocking pornography: “You don’t come to the library to look at porn and
stuff like that, do you?”.

User 2
Employed part time and studying part time, male, 0-19. Accesses the Internet at Chesterfield Library
every other week. He has the Internet at home and on his phone. He was not aware that the Internet
was filtered because he had observed that other Internet users accessed sites which he thought
were inappropriate. He had mixed feelings about filtering: “In some ways but not entirely. I mean,
like most filtering sort of software bans you from some sites like YouTube which people use a lot for
streaming their music but then you can kind of, then there will be other people, not to victimise
people, but you walk past and it’s kind of not what you want to be on in public. So, it’s just hard to
get the balance”.

User 3
Unemployed male, 50-64. Accesses the Internet at Chesterfield Library monthly and does not have
any other means of Internet access. He tends to use the Internet for work related information. He
had assumed that the Internet was filtered based on the AUP. He felt that filtering didn’t go far
enough: “Personally, from what I hear from the news, I think that a lot more stuff should be blocked,
yes I do”.

User 4
Unemployed male, 20-34. Accesses the Internet at Chesterfield Library weekly. He has the Internet
at home and on his phone. He was not aware that the Internet was filtered but agreed that it should
be: “I think in the same way that you wouldn’t have certain material on the bookshelves”.
**Case study 2: Edinburgh**

Researchers visited Central Library, City of Edinburgh Council where they interviewed seven members of staff at different organisational levels within the library service which sits within Services for Communities: the Digital and Information Services Manager, two Team Leaders and four Library Advisors. In addition, members of the public using the library PCs were approached and asked to participate in interviews. Six members of the public volunteered and were interviewed in situ. In addition to the online survey response completed by a senior member of the library service, a search of relevant documentation highlighted a number of local authority policy papers, web pages and other related literature which were also reviewed.

**Context**

Edinburgh is the capital city of Scotland and this unitary authority’s library service is home to 31 libraries including 27 community libraries. Edinburgh attracts a lot of visitors, including tourists, to the Central Library which is its busiest library. They typically come to access the Internet and print out airline boarding passes.

The People’s Network PCs were installed in Edinburgh City Libraries in December 2002, providing free Internet access to the public. In 2008, there were 320 PCs available for public use. Library users in Edinburgh presently have access to over 400 static desktop PCs which are installed with Microsoft Office. They provide free access to the Internet and in 2011-2012, offered a potential 794,647 hours of which 222,061 were recorded as used (27.9 per cent) (CIPFA 2012). Sessions are for one hour with two hours as the maximum. In order to use a computer for access to the Internet all individuals, including visitors, must join the library. When joining the library, under-12s are classed as children, between the ages of 12 and 15 as teenagers and 16s and over as adults. Library staff would expect children to be accompanied by an adult. The Edinburgh City Libraries’ website provides information for parents regarding Internet use and it states that when a child under the age of 16 joins the library their parent or guardian is asked whether they can use the Internet.

All library staff may assist the public with using the PCs. However, it is noted in the terms and conditions of use that this assistance is minimal: “Council Staff will try to assist users where possible but may not always be available to provided dedicated one-to-one assistance” (their emphasis). Complete newcomers to ICT are encouraged to sign up for LearnIT Computers for Beginners classes which are particularly popular with the over 50s. Demand is illustrated in the long waiting lists for these classes. These courses run at selected libraries for six weeks with each session lasting two hours. There are also LearnIT Beyond Beginners courses: five two-hour sessions based on a plan tailored to the user. There is also an I.T. Buddies scheme offering users one-to-one support of a one hour session for up to six weeks at a time with a volunteer. Six libraries have Libraries4U zones to encourage teenagers and young people aged 16 to 25 to use the library and its facilities including free Internet access.

Edinburgh City Libraries operate a matrix management structure. There is a strategic management unit which includes the Digital and Information Services Manager who reports to the Senior Library Manager. The libraries themselves operate on a neighbourhood level (there are five neighbourhoods) each led by a Partnership and Information Manager. Library Advisors may report to Team Leaders if there is an issue, alternatively they may go directly to the Digital and Information Services Manager or to the ICT Support Unit. The Digital and Information Services Manager, a senior member of library service management, has ultimate decision-making powers over blocking and unblocking of websites and liaises with colleagues in the libraries’ management team.
Managing Internet access

Edinburgh City Council use Blue Coat WebFilter software. The People’s Network PCs have always utilised filtering software. As the PN was being introduced, senior management members of the library service prepared reports for the council’s committees suggesting filtering software was installed, to which Councillors agreed. Filtering is explicitly referred to in Edinburgh’s ‘Internet and computers in libraries: Terms and conditions of use’ which is available on the council website, where it states, “All access to the Internet is filtered to prevent access to inappropriate material”. However, most of the users we spoke to in the library were unaware that the library employed filtering software. Filtering is based on websites categorised by a third party and “the Council cannot guarantee its absolute reliability or appropriateness” and as a result may be willing “on request, to release blocked material which users consider to be perfectly acceptable”. Indeed, a minority of Internet users do approach staff and inform them that a page has been blocked. Similarly, users are asked to let staff know if anything they consider unacceptable is accessible.

The terms and conditions are available online and include nine sections on access, availability, costs, assistance, information security, risk and responsibility, prohibited activities and review. They were last reviewed in 2010 when the service introduced WiFi. The information for parents also refers to filtering but points out that filtering is not a perfect solution: “Parents should be aware that no filtering system guarantees protection from viewing unsuitable material”. This pragmatic approach to filtering is reflected in the comments of management: “I think the important thing for filtering is that you have to be upfront to the customers, you have to explain clearly that you do operate filtering, and you will review anything which they either think should be available to them or shouldn’t be available to them. Every filtering system has significant weaknesses”.

WiFi is available in five libraries including the Central Library. WiFi access is filtered. When using the library’s WiFi connection, users see a special web page to log-on to before using the Internet, known as a captive portal. However, beyond this, management acknowledge that there is no way of knowing whether own device usage is appropriate.

Edinburgh utilise Netloan Internet booking software from Lorensbergs. In addition, visual monitoring of Internet use is perceived as important by management as a deterrent to misuse: “Our approach has always been to sight PCs in the way in which they are easily, relatively easily visible to staff and we do talk about physical monitoring as well”. However, front-line staff find that they have little time to undertake visual monitoring and are largely reliant on the filtering software to prevent misuse: “We have that many other things to do nowadays, it’s not as if we can sit there just waiting for the next thing to, ‘Oh, I’ll just keep an eye on that’”.

ICT support is managed by Edinburgh City Council’s Business Improvement Team. Library staff contact them primarily by email or by telephone about any issues which are then raised with the support company, Calyx Solutions. Frontline staff feel that the remoteness and invisibility of the support can be problematic at times and that library users respond more positively to specific rather than vague progress reports from ICT support. Internal ICT support work office hours, Monday to Friday. This can be frustrating for staff working in libraries open on Saturdays and in the evenings.

Ethical considerations

There were a range of views expressed by staff in relation to the ethics of filtering but predominantly, filtering was seen as something which was inevitable given that those viewing Internet content were doing so in a public space:
“I think inevitably when you are dealing with a whole community, you have to start thinking about if somebody was looking at a site which would be very offensive to another member of the community, I think you can’t just avoid the fact”.

“Well I think in the sense that it is a public space, I think that gives you that right to do that”.

Staff felt that it was important that library users had confidence in the library service and the use of filtering software helped facilitate this: “So I don’t think as a public body you can avoid trying to help people stay safe... People have to have confidence that you’re setting a little bit of a standard”.

“So unfortunately, yes, we do have to operate filtering systems...because it will give parents confidence, parents and carers confidence, teachers as well, for the offer that we have”.

**Managing misuse**

There have been no major incidents of misuse. Problems tend to be of an operational nature with users encountering network problems. Minor misuse tends to involve users viewing inappropriate images. On a couple of occasions library users have attempted to plug into the actual network. The terms and conditions of use state: “*Users must not connect personal equipment to data points on Council premises*”.

If misuse is identified a member of staff speaks with the library user initially. Perceptions of offensiveness are at the discretion of individual members of library staff. If a member of the public alleges that another library user is misusing the Internet, then it is investigated and if misuse is identified a warning letter is issued to the offending user reminding them of the terms and conditions of use. If misuse is persistent, Internet access may be withdrawn.

Copyright is implicit but not explicit in the terms and conditions of use: “*Users must not engage in activities that are illegal*”. The system is not able to identify breaches in copyright so is dependent on staff or other users noticing anything amiss. Management perceived that front-line staff are aware of copyright issues in general but not necessarily in the digital sphere: “I think that they will be focussing on more around what’s happening on the photocopier and the electoral roll than they will be on the PCs. They won’t really pick up a lot on that”.

File sharing is not permitted. The terms and conditions of use state that “*The Council automatically restricts or prohibits certain Internet-based activities and technologies, such as... peer-to-peer file sharing (e.g. BitTorrent)*”.

In relation to The Digital Economy Act, concern was expressed that as the service moves away from static desktop PCs to WiFi access, it may be more difficult for the service to monitor use. However, WiFi users access the network on a portal and therefore provide contact information in the form of an email address.

**Staff**

On a daily basis, staff switch the PCs on, register new users, manage bookings such as changing, creating, deleting and extending them over the telephone and in person. They also help the public use the Internet, troubleshoot problems, assist with printing, deal with complaints, switch the PCs off at the end of the working day, replace print cartridges and paper and report faults.

Staff receive minimal Internet training in their induction and staff have varying levels of ICT knowledge. Some staff undertook ECDL as part of the roll out of the People’s Network in the early
2000s whilst more recently staff have received training on the Netloan booking system. Staff knowledge of the filtering software utilised was negligible and some staff would have liked to know more about it, for example, what categories of content were filtered.

**Future**

Staff perceive that the library service still has a role to play in providing Internet access to those sections of the local population who still haven’t engaged with digital technologies and those wishing to use the Internet to apply for benefits now and in the future. This may require work with external agencies and volunteers to provide the kinds and depth of support required. Frontline staff felt that a lot of Internet users were unemployed.

It is anticipated that the increase in library users accessing the Internet on their own devices will continue and if not on their own devices, then using hand-held devices provided by the library. This would mean the library would need to consider offering the public the chance to print documents in the library using WiFi enabled devices.

**Users**

**User 1**

Male, employed part time, age 20-34. User 1 is able to access the Internet at home on a laptop and mobile phone but for the last six months has also accessed the Internet on the PCs at Edinburgh Central Library and usually does so on a weekly basis. He uses it to find information and maps. He was not aware that the Internet was filtered although it had prevented him from accessing some sites. He had mixed feelings about filtering perceiving that whilst having it may prevent system overload it could also prevent legitimate use: “Probably, to allow more people at the same time to use the Internet here probably filtering... especially streaming or downloading sites could be useful. But probably they should also allow for particular users because it’s happened to me that I needed access to maybe a file for example which, in the halls I live in, is not allowed, so in necessary extraordinary cases could be allowed”. He would prefer to ask a friend to access something for him at home rather than ask a member of staff to unblock a site: “Possibly, it could be a bit embarrassing but depending on the gravity of the situation...”

**User 2**

Male, full time student, age 17. He has been using his laptop to access the library WiFi for almost two months on a daily basis although he is able to access the Internet at home. He uses the Internet to work on past exam papers and to look at Facebook. He was not aware that the WiFi connection in the library was filtered: “So there are things that they just don’t let you on?” but felt it probably should be: “I wouldn’t not use the Internet because it’s filtered. Yes, they probably should filter it, just because... yes, I don’t have a problem with it and I’d say they might as well filter it”. He was not concerned about having to ask a member of staff to unblock in the future.

**User 3**

Male, self-employed, 35-49. User 3 has been accessing the Internet in public libraries for three years and uses his laptop to access the library WiFi, three to four days a week. He also has Internet access at home. He typically undertakes research for non-fiction books that he is writing. User 3 was aware that the WiFi was filtered and whilst he considered this may prevent the system from slowing down if too many users wished to access streaming services, felt that the controls should be relaxed a little as he was sometimes unable to access pages for his research: “Yes, I just tried to access something; it had a picture of a gun on it so I couldn’t access it but it was actually field sports”. User 3 was
unaware that he could ask for a site to be unblocked but felt in future that this was something he felt comfortable doing if required.

**User 4**
Male, employed part time, age 32. User 4 has been accessing the Internet on his laptop using the library WiFi on a daily basis for the last six months. He is also able to access the Internet at home. He uses the Internet for information, news, work and study and frequently accesses it for three to four hours a day. User 4 realised the WiFi connection was filtered as he was sometimes unable to download large files: “Sometimes I search some websites with books, big books or maybe PDFs and it’s true, some websites are blocked but okay, it’s not important to me”. He felt that it was reasonable for the library service to employ filtering on a technical basis: “It’s fair enough I think, it’s a good connection, I have never had problems”.

**User 5**
Female, semi-retired, 65-79. User 5 accesses the Internet at home and has been using it in the library on a fortnightly basis for the past year and a half. She is researching her family history and primarily uses the Internet in the library to access the Ancestry website. She felt that filtering was needed but hadn’t realised the library used filtering software to control content as she had never come across anything that was blocked.

**User 6**
Male, employed part time, 35-49. User 6 uses the library WiFi connection on his phone and laptop but does not have Internet access at home. He has been using the Internet in public libraries for ten years. User 6 uses the WiFi connection to look at social media sites and YouTube clips. He felt that libraries should filter the Internet and was aware that the connection in the Central Library was filtered. He was unclear what criteria were employed with regard to filtering and was not aware that sites could be unblocked upon request.
Case study 3: Brighton & Hove

A total of five staff were interviewed from Brighton & Hove library service. Researchers visited two of Brighton & Hove’s libraries: Jubilee Library and Hove Library where they interviewed four members of staff at different organisational levels within the Library Service: Library Community Engagement Manager, ICT Consultant, Library Officer and Security and Support Officer. A telephone interview took place with the Head of Service prior to the visit. In addition, members of the public using the library PCs were approached and asked to participate in interviews. Five members of the public volunteered and were interviewed in situ at Hove Library. In addition to the online survey response completed by a senior member of the library service, a search of relevant documentation highlighted a number of local authority policy papers, commercial web pages and other related literature which were also reviewed.

Context

Brighton & Hove is a unitary authority and city located in the South East of England. The authority is home to 14 libraries. The city’s main public library is Jubilee Library which opened in 2005 and is the second busiest library in England. Jubilee Library is open seven days a week. Hove Library, serving the west of the city, in contrast, is over 100 years old and opens to the public six days a week.

Library users in Brighton & Hove have access to approximately 180 static desktop PCs with Microsoft Office and free Internet access and in 2010-2011, were offered a potential 276,596 hours of which 139,387 were recorded as used (50.4 per cent) (CIPFA 2011). In order to access the Internet, adults and children including guests have to become members of the library and use their membership card and PIN. Guests may be issued with a temporary PC user card, which expires after a time, if they wish to check their email and cannot provide proof of address but are able to produce identification such as a bank card or bus pass. Free two-hour PC sessions are available at all of Brighton & Hove’s libraries except for Jubilee Library which offers one hour slots. Some libraries have drop-in PCs which are non-bookable and can be used for 15 minutes. Users may book the PCs in person with staff when they visit a library, on the telephone with staff or by using the electronic booking system at Jubilee and Hove libraries.

ICT support for the public includes one-to-one Silver Surfer sessions for the over 50s offering an introduction to ICT such as setting up an email account and Council Connect, providing free ICT sessions for residents of any age wishing to access Council services online. Nine libraries have Council Connect drop-in times offering 45 minute sessions with a volunteer whilst Silver Surfer sessions are held at three libraries. Silver Surfers and Council Connect sessions both use library volunteers.

Managing Internet access

Brighton & Hove Libraries provide filtered access to the Internet using Blue Coat WebFilter software which enables blocking by subject categories. Internet provision has always been filtered but in the early days of the People’s Network library personnel persuaded elected members to agree to relax the filtering levels as they were deemed too restrictive at that time to permit legitimate research by library users.

WiFi has been available at Jubilee Library since March 2013. The free WiFi connection is filtered and is managed via an external operator - The Cloud: “we are making it quite clear that it’s a privately provided service, it’s not a Council provided service”. Users accessing the WiFi connection log-on to a captive portal before using the Internet.
Brighton & Hove Libraries have an Acceptable Use Policy (AUP) which is available on the Brighton Royal Pavilion, Museums and Libraries webpages in the ‘Using Computers’ section. The AUP was reviewed in July 2010 in order to incorporate the issues surrounding users wishing to view live TV on the PCs which is not permitted as it would require the library service to have a television licence. It was also updated in July 2013 following the case study visit. The AUP is a one-side of A4 size document which states that whilst the library service provides Internet access it cannot accept any responsibility for content available on the Internet. The AUP clearly highlights that Internet content is filtered: “The Internet facilities are filtered, with a high level of filtering on the children’s computers and a minimal level of filtering on adult computers” but the software is not infallible: “no filtering software is totally effective”. Users are asked not to access material that is “Obscene, homophobic, racist or unlawful”, that is “pornographic or could cause offence to others” or “is in breach of copyright”. There was some suggestion by staff that users paid little attention to the AUP: “I don’t think a great many people actually read that. It’s the same with anything, any sort of acceptable terms. Who actually reads it?”

Children’s access to the Internet is managed by their membership details rather than on a PC by PC basis. This change was noted in the recent amendments to the AUP in which “filtering on the children’s computers” was replaced with “filtering for children’s access”. When they join the library, Internet access is not automatic for children under the age of 13 and requires permission from a parent or guardian. Filtering for children is at a higher level than for adults and teenagers, for example, they are unable to access information on lethal weapons. However, the filter does not block access to chat rooms and the AUP asks children under the age of 16 not to use them.

Library staff liaise with Corporate ICT who work with the Royal Pavilion, Museum and Libraries ICT team. Front line staff telephone ‘2001’ to log a problem with Corporate ICT where it is registered on a list and it then goes to the Libraries ICT team to be resolved. Staff in the Libraries ICT team are able to access user data logs if requested by the police or a library manager, for example. If a user wanted a site unblocking their request would move up the organisational chain to the Head of Libraries who would liaise with the Corporate ICT team. However, a Head of IT Security has recently been appointed and requests may go to them in the future.

Visual monitoring of Internet use by staff was seen by some staff as one way in which misuse could be minimised but there were diverging views on this amongst staff as not all of them felt this was either appropriate or possible:

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

“I mean we haven’t got the staff time really to be monitoring what everybody’s using”.

**Ethical considerations**

Staff generally agree that filtering is necessary with a minority expressing some reservation. This was rationalised as libraries having a responsibility to library users to protect them from dangerous material in a public space and to safeguard families in particular who have a high level of trust in the service:

“We’re just trying to prevent sites from being accessed that could cause offence to other people”.
“I see the balance. It’s the usual thing. The small percentage if they were allowed to spoil it for the majority... I think that’s [filtering] a way of levelling the playing field because the great majority are not actively looking for terrorist sites or whatever or paedophile sites. Those that think they can get away with it hopefully will be filtered out”.

“I think it’s necessary, I do, actually. We have had issues around people trying to access certain sites and some of the sites that they’ve accessed have been quite inappropriate especially when you’re sitting in a public building”.

“Well in my view, regretfully, I think it is necessary to have a level of filtering but only a minimum level of filtering that is sufficient to protect the public from some of the more offensive and dangerous material that is out there”.

**Managing misuse**

Most staff agreed that there were no major misuse incidents but there were some minor ones: “I’ve not come across it massively. In five years I’ve only had to call up one person”. Examples included an individual who plugged a device into the network in order to hack the booking system. One member of staff had challenged a man watching a film in the library which contained nudity: “I said ‘sorry you can’t watch that here’ and he said ‘but it’s comedy’ and I said ‘I don’t care if it’s comedy, it might be a very funny film but you can’t watch that here’”. Another member of staff related an incident where a user had been looking at necrophilia websites.

At senior management level there was some indication that there had been a small number of major incidents in the past which had involved the police: “And we have had incidents over the years where people have been looking at pornography or have managed to get around the filters, as we know they are not infallible, and I think we have even participated and supported prosecution of some people as a result of that”.

There is a range of sanctions that the service may implement if library users breach the AUP including blocking an individual’s library membership card. Users found to be in breach of the AUP are given the benefit of the doubt the first time, for example, if they open an attachment which contains offensive content: “But it’s very rare that we would block somebody’s IT use”. Staff are not encouraged to confront a user if they suspect that they are viewing illegal or offensive content but are urged to make a note of it and liaise with ICT staff who may then check the user log: “The staff do monitor but we advise them not to wade in, to report it upwards rather than trying to tackle it directly and just to check in on the best course of action if they suspect something”.

Staff have not received many complaints about the filtering software, one member of staff noted that: “I haven’t had anybody say ‘It’s not fair. I can’t look at this’ which is what I think would be my first, ‘hang on a minute is it too heavily filtered?’” whilst a member of ICT staff, having more of an overview of the numbers of complaints noted, “There have been occasions when there has been a site where somebody says ‘I don’t think this site should be blocked. Could you have a look at it?’ But we will have a look at it in that case and if it’s deemed that it’s actually a mistake that it’s blocked, we will unblock it”.

In relation to online copyright there are notices in the libraries and it is mentioned in the AUP which users must agree to before using the PC; users are asked not to access material which “is in breach of copyright”. This was recently updated and “including watching films (on disc, downloaded or broadcast)” was added to the AUP. “I think the one thing that they do notice is trying to download things like certain software and even we can’t access that, it has to all come through ICT”.

However,
it was perceived that staff awareness of online copyright did vary: “they know generally about maps and things like that... but I doubt if they’d know copyright law around the Internet”.

The service are confident that they will comply with the DEA and its implications will be considered organisation-wide: “We’ll be looking at it corporately, partly because it’s not just libraries now that are providing the public with access to IT but when the Act came in we took advice and we are fairly confident that we can comply with it”. It was argued that because users must be members in order to access the Internet and provide their address details as well as access being logged against activity, the service would be able to meet any obligations. In addition, users must agree to the terms of the AUP when they begin their Internet session. Externally provided WiFi means that the library service is not responsible for what people access when using the WiFi connection.

Staff
Staff perform numerous tasks on a daily basis to facilitate Internet access for the public. These include turning on all the PCs, booking machines and printers and ensuring that there is enough paper for the printers. Other tasks include registering new members with the service, troubleshooting when library users encounter PC problems, showing users how to print from the PCs is centralised with a queuing system and how to use the self-service booking machine.

At Jubilee Library there is a dedicated IT suite with approximately 30 PCs. There are no longer staff dedicated to the suite but there are members of staff on that level of the building who can be tracked down by radio if needed in the suite.

Staff receive induction training when their employment with the library service commences which includes an element of supporting Internet users.

Issues
Expectations are being placed upon Brighton & Hove libraries as they are suggested as the place to go for Internet access by some Job Centre staff: “A lot have been sent through from the Job Centre”. This was echoed by one of the users: “The Job Centre directed me to come over to use the library as a resource to help me with any researches or applications online”. Unfortunately, staff are unable to provide dedicated one-to-one support with job applications. Council Connect is helping to fill this vacuum. As a member of staff observed, the Internet was crucial in the library because: “It’s [Internet access] what’s needed the most because you have to do everything online now it seems”. The Library Community Engagement Manager is currently working with other council departments such as Housing as part of a bid to get council tenants online. The Head of Service was clear that they had to address this agenda: “the provision of information is part of our statutory duty and nowadays information is very largely digital, therefore, there is a very clearly a statutory requirement for public libraries to be involved in public access to the Internet and supporting people using the Internet effectively”.

Future
Staff in Brighton & Hove felt strongly that there was still great demand for Internet access from users now and in the future as a member of staff at Hove library described:

“When there’s an outage, a few weeks ago there was no Internet for the whole day and it was bananas in there. It was like ‘somebody’s taken away my lifeline. When’s it going to be back on?’ and also we’re not open on a Monday morning. Monday afternoon I now call it Manic Monday because people are queuing up the stairs to get on the computers because they haven’t had them
on Sunday and Monday morning so it’s almost like a fix, a drugs fix... You notice it, when there’s no Internet access, the library goes quiet”.

“I would say that a very high percentage of people that come in and join up are predominantly PC users now”.

**Good Practice**

A combination of filtering software predominantly, an AUP which is regularly updated to incorporate changes in use, staff vigilance and user authentication enable the service to best manage Internet use by the public: “Mixture of measures including User ID and filtering” (survey comment).

**Users**

**User 1**  
Male, unemployed, 26. User 1 usually accesses the Internet on a daily basis at Hove Library and does not have any other means of Internet access. He was directed by the Job Centre to use it at the library to search for job vacancies and submit online job applications. He was not aware that the Internet connection in Brighton & Hove was filtered but felt that it was appropriate as public libraries are places of learning. However, he felt that asking for a site to be unblocked might be awkward.

**User 2**  
Female, employed full time, 21. User 2 usually accesses the Internet on a daily basis at Hove Library although she also has Internet access where she is currently residing. She is working as an au pair and uses the Internet to study and listen to music. She wasn’t aware that filtering was used and felt it was a good thing to have in a public library but did not know what would be blocked. She would not find it difficult to ask staff to unblock a site but appreciated that some people might find it uncomfortable.

**User 3**  
Female, retired, 65-79. User 3 accesses the Internet on a weekly basis at Hove Library and does not have any other means of Internet access. She uses the Internet to contact friends, news and for leisure. She was aware that the library employed filtering because it was mentioned on the Acceptable Use Policy which she usually reads when she uses the PCs: “Definitely. Because some things are legal to look at and some things are not” and felt strongly that the Internet should be filtered: “I feel sometimes I have been quite shocked by things that I’ve seen and I don’t want to”.

**User 4**  
Male, unemployed, 35-49. User 4 accesses the Internet on a daily basis in libraries across Brighton & Hove and does not have any other means of Internet access since he moved back to the UK three months ago. He primarily uses the Internet to search for jobs and also for recreational use. He agreed that the library should filter Internet content and had assumed that it probably did: “I think they should filter as the Internet is used by everybody”.

**User 5**  
Male, unemployed, 35-49. User 5 accesses the Internet twice a week in the library for recreational purposes. He also has access where he is a volunteer and at a family member’s home but does not have Internet access himself: “I prefer to use it at home but it’s lack of money. I can’t... it’s not a necessity at home”. He was unclear what filtering software did and hadn’t realised that it was used at the library. Neither was he sure about whether it should be used. He felt that there were some political sites he would quite like to look at but was worried that they may be blocked: “It’s risky doing that”. He would be concerned about asking a member of library staff to unblock a site.
Case study 4: Northern Ireland

Researchers visited one of Libraries NI’s Regional Administration Centres and a branch library where they interviewed six members of staff at different organisational levels within Libraries NI: an Operational Manager, e2 Project and Service Manager and e2 Project Officer at the Admin Centre and two Branch Library Managers and a Library Assistant at a local branch library. Members of the public using the library PCs were approached and asked to participate in interviews and six volunteered to take part and were interviewed in situ. In addition to the online survey response completed by a senior member of the library service, a search of relevant documentation highlighted a number of local authority policy papers, news stories and other related literature which were also reviewed.

Context

Libraries NI (the Northern Ireland Library Authority) was established in 2009. It took over the public library function of the five Education and Library Boards of Northern Ireland. Libraries NI is responsible for 98 libraries including 96 branch libraries and two central libraries (Belfast and Derry) as well as a number of mobile libraries and Homecall Service vehicles.

Structurally, Libraries NI is headed by a Chief Executive supported by two Directors – Library Services and Business Support. Within Library Services, the Director is supported by four Assistant Directors each with their own geographic area – A, B, C or D. The Operational Manager we interviewed, for example, reports to Assistant Director A and has responsibility for a number of Area Managers who manage the Branch Library Managers. The Director of Business Support is supported by four managers including the Head of ICU/ICT who is responsible for ICT and Information Management Services, the Electronic Libraries for Northern Ireland Project and now the e2 Project (a new library ICT infrastructure implementation and management project). The e2 Project and Service manager we interviewed, for example, reports to the Head of ICU/ICT.

The People’s Network was launched in November 2002 in Northern Ireland. A PFI contract between the company, Amey, and the NEELB (North Eastern Education and Library Board) on behalf of the five Education and Library Boards for the Electronic Libraries for Northern Ireland Project (ELFNI) was signed in early 2002 which included the People’s Network and a single Library Management System across the five Boards. The implementation of ELFNI as it became known began in May 2002. According to 2012 figures from CIPFA, public library users had access to a potential 3,187,802 hours on public access computers in Libraries NI (1st April 2011 to 31st March 2012) of which 33.0 per cent were used (1,053,189) (CIPFA 2012).

ICT support for the public includes computer classes which are free to library members, designed in-house by Libraries NI Learning and Information Team and delivered by frontline library staff: Got IT? and Go ON. Got IT? is an introductory course aimed at adults new to using computers and the Internet whilst Go ON is designed for those wishing to further develop their ICT skills. The latter includes modules, available at 98 libraries and as outreach including ‘shopping online’, ‘editing digital photographs’, ‘travel’, ‘social networking’, ‘get that job’ and ‘organise your life online’.

Libraries NI offers primary school children a series of three class visits to their local library of which the third visit includes computers, using the Internet in the library and e-safety.

Managing Internet access

In order to access the Internet for free on PCs, adults and children must be members of the library. Visitors, however, need to provide some form of identification and pay for use. Library members receive a Personal Identification Number (PIN) when they join the library which is required in conjunction with their membership number in order to access the Internet. Members may book the
PCs for up to 60 minutes at one time although they may use the PCs for longer if there are no other bookings whilst visitors are limited to 30 minutes. PCs may be booked online using the Pharos booking system, in person in the library or by telephone.

Children are also required to have their membership number and PIN when using the Internet. Parental permission is required for Internet access up to the age of 16. Content is filtered at a higher level than for adults. Under 16s are unable to access social media sites such as Facebook in Libraries NI. In most libraries, as far as is practicable, PCs for adults and children are sited away from one another: “With computers they would be at opposite ends of the library just so there isn’t any opportunity for a child to see something that an adult’s possibly looking at”. Libraries NI’s approach to children’s use of the computers and the Internet is heavily influenced by child protection concerns. The e2 Project Officer we interviewed is also the Child Protection Officer for Libraries NI whose role includes responsibility for the ‘Conditions of Use’ policy for the Internet.

Libraries NI currently use WebMarshal filtering software across the network. This will soon be replaced by the Websense filtering solution. Fujitsu were awarded a five year contract in 2013 to replace and manage the ICT infrastructure in Libraries NI (known as e2) taking over from Amey Plc who managed the infrastructure from 2002. WiFi Internet access is also filtered. At present only three libraries provide WiFi but in January 2014 as part of e2 it will be rolled out across the entire network of branch libraries. In order to use the WiFi connection library members and guests need a username which is given to them on a voucher from library staff. Once e2 is implemented members will need to use their borrower number and PIN to use the WiFi connection, however, all WiFi access will be filtered at the same level that is used for children: “The only difference being because I have no control over where you sit in the library as an adult you will be filtered as a child if you’re using your own device just because you could be sitting beside a child. With children the restriction levels are different. In my mind it will work two ways, people will be happy enough to use their own devices but there will also be genuine sites as well that they can’t use just because filtering blocks it so it will also keep people wanting to use our computers as well. But it’s safer to have the same level of filtering” [e2 Project and Service Manager].

While Internet access for children has always been filtered, Internet access for adults has changed over time:

“We’ve had a time when we had filtering for both adults and children. Then we’ve had a time when we’ve only had filtering for children and now we’ve reverted again to having filtering for adults and children. So we’ve always filtered for children but we’ve varied in what we’ve done with adults”.

The Acceptable Use Policy for public computer use is known as the ‘Conditions of Use’. The policy was last reviewed in May 2012 and is available on the Libraries NI website. The details are also available online in ‘Library Computers Acceptable Use Guidelines’. There is a section aimed at Adults (16 plus) and Children (under 16s). It is stated that adults may not use the computers to: “Access, view, download, display, copy, create, store, transmit or publish any material that constitutes pornography or which is unlawful, pornographic, obscene, paedophilic, racist, abusive, defamatory, violent or which otherwise could reasonably be considered offensive” (p.4) and in relation to copyright states “You must not download any software to the computer or violate copyright or software licences” (p.4). The section aimed at children notes in its introduction that Internet access is filtered and in relation to children under the age of 8 specifically, “Although we are using filtering software for children we cannot guarantee that it will be totally fool proof” (p.10). Children under the age of 8 are not permitted to use the computers and access the Internet unless accompanied by a parent or guardian.
When accessing the Internet in the library, users must agree to the Conditions of Use on the log-in screen on the PC before they are able to proceed. However, staff were not confident that users paid much attention to the wording of the policy: “I suppose there is a wee Acceptable Use Terms and Conditions comes up but to be honest most people just click past that” [Branch Library Manager].

**Ethical considerations**

Filtering is mostly perceived by staff as a pragmatic tool required in order to protect children and adults from accessing potentially harmful content on the Internet. Staff did not feel there were any ethical inconsistencies in having filtered content:

“We as staff prefer it filtered”.

“What people do in their own homes is fine but in a public place there needs to be some control I think”.

“Personally, I think that it needs to be restricted”.

“I don’t have any ethical issues with filtering. I think it’s something we do need to do”.

One member of staff highlighted that whilst public libraries stock some books which include text of an erotic or sexually explicit nature, visual depictions are banned:

“So we can have books on our shelves that are very sexually explicit verbally and we’ll not censor that but if you depict those same verbal descriptions visually, we will censor that. So there’s a wee bit of a double standard in there but we’re a public service and the people who frequent our libraries are from a few months old to in their 90s, so we make adjustment accordingly”.

Most of the library users interviewed were aware that the service may use filtering: three were not sure, two were aware that it was filtered because of their experiences when using the Internet and one was not aware. The protection of children emerged as a prevalent concern but there were some reservations about its use:

“Some people find things offensive that other people don’t so you have to weigh the pros and cons up. You know, both sides. But definitely for children, yes”.

“They should block maybe some porno sites or something for the kids... maybe. Or maybe to ask if they are 18 or something? Otherwise I think they have no rights to block”.

When asked how they would feel about asking staff to unblock a site most of the users questioned would feel comfortable about approaching staff and some had done in the past:

“If it was legitimate. Oh yes, say you were looking up, as I’m going to in just a minute, if there are any jobs going at Christmas time at Marks and Spencer and I can’t find that, I’d be certainly asking”.

Two users said they would feel uncomfortable and would not ask:

“I’d feel awkward. I’d just carry on and leave it”.

“No I wouldn’t. I would just not go there”.
Internet users may ask a member of staff in the library about unblocking/blocking a site or they can email the library service. The decisions about sites to be blocked or unblocked are made within the library service. Front line staff can pass on details of sites to their Area Managers who make the decision about that site and request ICU to block or unblock it: “So it’s a fifth tier officer who takes some of the decisions about what sites can be blocked. So fairly well down I suppose”. However, filtering levels are generally managed by staff in ICU. When the Acceptable Use Policy was last reviewed some amendments were made to adult filtering categories which had such a big impact on the system, additional servers were installed: “WebMarshal has a category just for pornography so basically when you were ticking that you were ticking their recommendations over and above what we had already asked to be blocked so I suppose it was using their database and using their experience. It was blocking a lot of sites. It would probably have covered some of the peer-to-peer sites as well and all that sort of stuff so it was a big change. It was, I’ll be honest, the first couple of weeks you were switching it on and you were seeing what the impact was on the network and you were maybe switching it off for a few hours to go away and assess because it was, it was slowing things down. In the end we actually ended up putting additional servers in”.

Managing misuse

Staff interviewed could not recall any major incidents of misuse, however, one member of staff made reference to an incident which had led to police prosecution.

Anecdotes relating to misuse were generally historic ones: “When we first got our computer suite in and that would have been... almost 10 years but when we first had our computer suite in that would have been in our old library...there was a lot of problems then... Probably photographs and just silly things like that. Most were younger boys you know that thought this was very funny” [Branch Manager]. Staff were aware of occasional minor breaches such as users accessing inappropriate images in the library but these were infrequent: “It happens now and again. Because we don’t always see what they’re watching now and again it has been a problem” [Library Assistant].

The Libraries NI Annual Report for 2011 to 2012 refers to two court cases of misuse which occurred in libraries prior to the establishment of Libraries NI in 2009. The Chief Executive of Libraries NI noted that “Libraries NI facilitates approximately 1.5 million computer sessions for the public each year. With this volume and the technology available, there is a risk that a few instances of misuse may occur which could damage the reputation of Libraries NI” (p.50).

A three-stage process is in place to deal with misuse. Adults are given three opportunities to stop misusing the service before a three month ban is imposed. Children breaching the Conditions of Use are firstly given verbal guidance followed by a verbal warning. Finally, a letter is sent to their parent/guardian advising them that they are banned from using the Internet for one month. Bans are rarely imposed: “We do ban people from time to time. I wouldn’t say it was a huge amount of people but we do ban people from using the Internet because of misuse”.

None of the staff interviewed were aware of any online copyright infringements. The filter prevents peer to peer file sharing. However, one member of staff did notice that library users sometimes attempt to print out album covers which they assumed meant that they were copying CDs: “The odd time people try to print out CD covers. We get that so they’re obviously copying CDs or DVDs and then want to make it look good so they’re trying to get the printouts and they ask us to help them. It’s a bit of a grey area. Some staff think ‘well it’s up to them what they do’. Other staff say ‘well that’s illegal so I’m not helping you’. We probably should be saying ‘that’s illegal, I’m not helping you’... I’m not actually sure if that is written down somewhere from a copyright point of view...”
Staff
To provide Internet access frontline staff switch the PC monitors on, deal with bookings in person and on the telephone, take payment for print outs, support users with training sessions, perform basic troubleshooting and liaise with branch library managers when there are any issues they cannot resolve. Branch managers would firstly contact the Fujitsu help desk directly if there were hardware or connectivity issues. They might also contact the Project and Service Manager at the ICU.

Staff received training as part of the NOF ICT programme – the ECDL (European Computer Driving Licence), Office 2010 and were offered training in Got It? but according to one member of staff, they have not undergone any recent Internet related training: “We did have very, very basic training when they introduced Windows 10 [sic] but basically it’s on the job learning. You learn by doing it yourself you know and the training that we got was very minimal. Very, very basic”.

A pertinent issue appears to be users asking staff to assist with online purchases which they are not permitted to do:

“The other thing is if they’re paying for things on their credit cards we’re not allowed to help in case”.

“People’s bank details which we don’t want to know and we’re not supposed to but they’re pressurising us to do it because they can’t do it themselves. That’s quite hard on the staff. I would put my foot down and say ‘no we’re definitely not doing that’ because if anything goes wrong they can come back and say or if something happens to their bank details they could say ‘oh I gave it to that girl in the library’ so we would be quite strict with staff and they would all say ‘no we’re definitely not doing that’”.

Users sometimes have high expectations of the levels of ICT skills staff possess which they are not always able to meet as this library assistant highlighted: “They think well ‘how do you upload a picture from Facebook?’ We don’t always know the reason for that”.

Future
Staff in Libraries NI felt it was important to continue providing the Internet particularly for adults and children who do not have Internet access at home:

“Well there’s an awful lot of people who don’t have access at home. We get a lot of single people on their own living on benefits and having Internet access at home is maybe a luxury that they can’t afford”.

“Socially I think there are a lot of people out there who use us. We’re the only contact that they have in a day and they don’t have a computer at home, they’re never going to be able to afford to get BT in for the broadband or whatever. I’m thinking in particular of somewhere like Belfast Central where we have a lot of computer users who would be in that position”.

There was also a feeling that the introduction of WiFi across Libraries NI might result in a different cohort of users accessing the Internet in a public library:

“I think it’ll be more than the people who come in to use our computers because that’s what people expect now. Plus people want to lounge in a chair and look at their I-Pad”.

Good practice
In order to manage Internet use effectively, Libraries NI rely on filtering software in conjunction with an AUP which is regularly reviewed by Library Services staff. In terms of reacting to user and staff concerns about appropriate content, Libraries NI appear to benefit from a close working relationship between Library Services and ICT/ICU within Business Support with Librarians making judgments about sites to be blocked and/or unblocked which ICT/ICU implement.

Users

User 1
Female, 50-64, unemployed. User 1 is partially sighted and accesses the Internet on a daily basis at her local public library. She does not have Internet access at home and has been using it in her library for more than a decade. User 1 uses the Internet to check her email, access social media sites such as Facebook and purchase items online such as flights. She is aware that the Internet is filtered because of the Conditions of Use and feels strongly that it should be in order to protect children. User 1 is quite happy to ask staff for help and wouldn't feel awkward if it was in relation to something that the filter had blocked. User 1 is quite happy to continue accessing the Internet in the library as it is important for her to have an activity which involves leaving her home every day and prevent isolation: “Everybody keeps saying just get a laptop but that means you’ll be sitting in the house. You’re better sitting in the library and you can maybe even get talking to somebody”.

User 2
Female, aged 27, unemployed. User 2 comes to the library to use the Internet every week. She tends to use the Internet to search for jobs, look at Facebook and Twitter and occasionally watches television. User 2 suspected the Internet was filtered but perceived filtering positively: “I’d an idea that they do filter a lot of things”. She still envisages herself coming to the use the Internet in the library even if she finds paid work: “Hopefully if I get a job I’ll be using it for work and stuff”.

User 3
Male, aged 41, disabled. For the past four years, User 3 has been coming to the library to access the Internet. Although he can access the Internet on his mobile phone he doesn’t have an Internet connection at home: “I’ve got it on my phone but we don’t have a computer or anything else in the house. We don’t have a phone line in the house even”. Without free access at the library he couldn’t afford to use the Internet: “If it wasn’t here or it wasn’t free I couldn’t afford to use it. I think it’s a great service”. He tends to come twice a week to the library to shop online, watch content on YouTube and look for genealogy records. User 3 was aware that the Internet in the library may be filtered: “Just always assumed it was filtered for safety” and agreed that it should be especially in relation to children but noted that offensiveness was subjective: “There’s some music videos and stuff you would get on YouTube that I think would be offensive to some people. Some people find things offensive that other people don’t so you have to weigh the pros and cons up. You know, both sides. But definitely for children, yes”.

User 4
Female, 20-34, currently on maternity leave. Although User 4 is able to access the Internet at home she uses the library PCs about once a month, usually to print something out. She tends to use the Internet for research and study in the library whilst at home she would perhaps view streamed content. User 4 was not aware that filtering software was used by Libraries NI but reflected that the service probably should filter some content particularly in relation to children: “Why not, yes. Probably they should do. I never thought about that before... They should block maybe some porno sites or something for the kids or something, maybe. Or maybe to ask if they are 18 or something?”
Otherwise I think they have no rights to block”. User 4 felt that if she came across something that was blocked she would not feel comfortable asking staff to unblock it: “No I wouldn’t. I would just not go there”.

**User 5**
Female, retired, 50-65. For the last six months User 5 has been accessing the Internet at her local public library usually on a fortnightly basis. User 5 likes to search for holiday information, book flights and search for job vacancies online. She doesn’t have Internet access at home. When asked about filtering, User 5 assumed the library Internet was filtered but did not know for certain: “I would have assumed so. I didn’t know but I assume so”. She felt strongly that filtering should be used particularly in relation to social media: “I don’t like to use the words because it’s going to be on the recording, you know what I’m talking about, in fact, all that stuff should be took off and that Facebook should be more monitored as well”. User 5 would be comfortable asking staff for help if a site she wanted to view was blocked and has asked them for assistance in relation to Internet access before. She expressed some reservations about the proximity of the PCs to one another: “I think they’re far too close together. You could look over and see... say you wanted to look up something of a sensitive nature, say medical things or to do with court that type of thing, you really wouldn’t want somebody looking over your shoulder, glancing over because I’ve done that myself sometimes and you have to prevent yourself from doing it. They could be a wee bit more private. Spaced out a bit more”.

**User 6**
Female, 35-49, full-time Mum. For the past year, User 6 has been accessing the Internet at the public library. She tends to use it to look at Facebook. She became aware of filtering when she tried to visit a website using her daughter’s log-in and it was blocked: “I used my daughter’s card for Gumtree and because she’s under 16 it wouldn’t let me on and then they said ‘it’s blocked’ because I’d lost my library card and was trying to use hers”. User 6 felt that maybe more content should be blocked but wasn’t sure why the service employed filtering. She said she would feel uncomfortable having to ask staff to unblock something for her. User 6 felt that being able to access the Internet was crucial since more and more services were accessed online: “Well the Internet’s coming for everything now, isn’t it? You can do anything on the Internet so somebody I know does online banking on the Internet so I think we need the Internet basically”.


Case study 5: Merthyr Tydfil

Researchers visited Merthyr Tydfil Central Library in Wales where they interviewed seven members of staff at different organisational levels within Merthyr Tydfil County Borough Council: an Operations Librarian, Assistant Librarian, two Members of Support staff, two Library Assistants and a Desktop Services Engineer. Members of the public using the library PCs were approached and asked to participate in interviews and six volunteered to take part and were interviewed in situ. In addition to the online survey response completed by a senior member of the library service, a search of relevant documentation highlighted a number of local authority policy papers, news stories and other related literature which were also reviewed.

Context

Merthyr Tydfil is a town in South Wales administered by Merthyr Tydfil County Borough Council. There are four libraries in the borough; Merthyr Tydfil Central Library is the largest and there are libraries in nearby Dowlais and Treharris as well as a community library which has recently opened in Aberfan in a community centre. There is also a mobile library and a Home Links Service for housebound members of the public.

Structurally, this small library service consists of the Head of Libraries supported by four Operational Librarians under which sit Member Support; supervisory staff who manage Library Assistants. The Desktop Services Engineer is also employed by the Borough Council but sits within the corporate IT team. The IT team look after the hardware infrastructure which includes web filtering and liaise directly with library staff.

The People’s Network was launched in Merthyr Tydfil libraries in 2002 at the same time as its first library management system went live. The latest completed CIPFA return for Merthyr Tydfil is the 2010-11 return which states that there were 80 terminals in the borough providing access to the library catalogue or to the Internet and of a potential 104,802 hours available on the People’s Network PCs, 19,196 were recorded as used (18.3 per cent). According to more recent figures from the Welsh Public Library Performance Indicators, the take-up of public access PCs has increased in Merthyr Tydfil from 18.3 per cent in 2010/11 to 23 per cent in 2011/12 to 40 per cent by 2012/13.

ICT support for the public includes immediate, short-term support from counter staff helping users log-on for example but those requiring more detailed support are signposted to the training sessions offered in the libraries. Working in partnership with community organisations, the library service provides drop in sessions and a Job Club at the Central Library. A local college facilitates ICT sessions for beginners at Dowlais library. Staff perceptions of Internet use in the libraries by adult users include social networking, playing games and searching for jobs whilst recently noted activity includes users wanting to download the self-certification form from the government website, GOV.UK in order to claim statutory sick pay. Staff observe that children tend to use the Internet in Merthyr Tydfil public libraries for homework purposes.

Managing Internet access

Internet access is free for members of the library service who need a borrower number and a PIN/password. Guests who are able to provide some means of identification are given a temporary log-in.

Internet content is filtered and filtering software has been in use since 2002 when the People’s Network computers and the library management system were introduced. Certain categories are blocked for all users including sexual content, violence, extremist, intolerance/hate, bad language,
file sharing/peer to peer, gambling, hacking, weapons, illegal drugs, spyware, criminal skills and proxy avoidance.

Access protocols for children have recently changed and the age of children requiring parental permission to use the Internet has been lowered from 13 to eight. Rather than asking parents whose children are joining the library for permission to use the Internet it is assumed that they are permitted to do so unless the parent decides to opt them out.

The Acceptable Use Policy is currently under review. It is brought to library users’ attention when they join the library and every time they use the library PC. The full AUP is available on the libraries’ website to download. Filtering is explicitly mentioned: “Users must agree to use computers protected by software that filters content and restricts access to some material and must make no attempt to remove or alter such safeguards” (p.2). In relation to content it is clearly stated that users must not intentionally visit sites that contain sexually explicit, violent or offensive or illegal material (p.3). If users “unintentionally visit any sites that are explicit, violent, offensive or illegal” they must inform library staff (p.3). There is some flexibility within the AUP as users may be able to visit prohibited sites if they can demonstrate to staff that it is for professional or study purposes (p.4).

**Ethical considerations**

The majority of staff interviewed felt that it was ethical to filter Internet content because libraries are public spaces for all members of the community and the protection of minors is paramount:

“Yes, I do. If they want to view things like that, do it in your own home”.

“I can have an eight year old sat next to somebody. There needs to be some filtering to protect those people”.

“Obviously it’s a sensitive area. We’ve really approached it from the angle that we’ve got to strike a balance really between educational aspects and obviously things that are undesirable”.

However, it was acknowledged that, ideally, information should be freely available and the public library might be your only point of access: “You should be able to search for whatever you want to find”.

Filtering software was introduced in 2002 and has recently changed from Websense to Palo Alto. The decision to switch suppliers was made by IT. Library staff told us of a number of instances where users are finding that sites they could previously access are now blocked, for example:

“Suddenly sites that people have been accessing like the Royal Artillery site where somebody’s doing family history research and they’re looking at the museum and that was suddenly blocked because it was artillery”.

Staff had to deal with library users expressing their dissatisfaction with this change: “Yes, they’re [the users] not happy at all because they see it as a kind of infringement of their ability to use the web”.

Over blocking is experienced by one library user in particular who finds numerous sites are blocked when she is using the Internet including some employment sites: “I’ve been on the web looking for jobs and they are blocking things that are just totally legitimate and there’s nothing, no reason that they should block them” particularly in recent times: “Well it wasn’t so bad it’s only since they’ve updated their security system and it’s got a lot worse lately”.

Managing Access to the Internet in Public Libraries [MAIPLE]
For sites to be unblocked staff contact the IT team via email or telephone and request that it is unblocked. Ultimately, decision making rests with the local authority’s corporate IT team. However, staff perceptions of the ease of this process did vary somewhat from “that was just a phone call or an email to X and he releases it” to having to “nag IT department” to unblock a site. It wasn’t always clear from our interviews that sites would be unblocked even if they were legitimate:

“Up in Dowlais there are certain sites that you can’t get on and they’re innocent sites. There was one gentleman who said he listens to military music – well, they stopped that site. Well I phoned up IT to ask them and they said ‘well what it is, due to our new filter system, there’s certain sites that can’t be accessed’ and they said ‘there is nothing we can do about it’.

Users may be given access to a certain site for a short time: “If a member of the public makes the library staff aware of that, then they’ll contact us, or myself and we’ll just take a quick look at the website and see if it’s wrongly categorised for instance, then we’ll take action accordingly. We’ll either unblock it or we give a reason why we would be unable to do that...I could give them access for a couple of hours and they could get what information they needed from there and we could re-block it, if it was deemed necessary that is”.

The perceptions of library users in relation to asking for a site to be unblocked also varied. Only two of the six users we interviewed would be prepared to speak to a member of staff about it.

Managing misuse
Staff recounted only one recent, major, incident of misuse when it was discovered that a user was illegally downloading films in the library: “He’d managed to override the security system and he was there for two or three hours and we didn’t realise then that he was downloading films and then he’d go home and probably download them onto a disk and sell them”. The AUP states in relation to content and use that users “must agree not to infringe the copyright of another person” (p.3) and “must not copy or distribute restricted material without permission from the copyright holder” (p.7). The web filter is configured to prevent file sharing or downloading of materials: “The ports that would enable things like torrents and specifically file sharing applications are blocked through the network so they wouldn’t be able to use that sort of angle” but as staff were aware, this had not stopped this particular user from illegally downloading films: “I have recently banned a gentleman for doing it, I informed IT at the time because he was downloading them for commercial use and I caught him and we followed the history of what he had been downloading and when he came back in to use the computers later on, I told him he was banned from all of Merthyr libraries and not to come in again and ask to use the computers because we knew what he had been doing”.

When questioned about the Digital Economy Act the member of IT staff felt confident that the service was well prepared for the Act since users are unable to download or share materials. Use is monitored and users breaching the AUP will be punished: “Well there have been, as far as the port blocking is concerned. Harsher penalties we’ll say if somebody is blatantly caught using a file sharing programme or a website then they run the risk of them losing their access to the public machines, and that can be traced if we are made aware of it”. Senior library staff were happy to let IT implement the appropriate solutions so that the service was complying with the law.

In extreme circumstances staff do ban users and they may also close user sessions on a PC if they feel they are in breach of the AUP: “Put a message on their screen and close the computer down which has probably happened once or twice”. This penalty is noted in the AUP where staff may ask users to close sites that are in breach of the AUP (p.10). Users’ access might also be suspended or they might be banned from accessing the Internet in the library. In extreme cases the police would
be involved. As the AUP explains: “Other sanctions may apply in addition to a loss of privileges, including criminal prosecution” (p.10).

Using the iCAM system, staff are able to monitor what users are doing. iCAM Workstation Control also includes an electronic booking system for the PCs in Merthyr Tydfil Central Library. Monitoring of ICT facilities is noted in the AUP: “All users must agree that County Borough Council staff will monitor their use of ICT facilities” (p.1). However, this is to be undertaken with sensitivity: “Library and other staff monitoring the use of equipment will respect the privacy of legitimate users at all times” (p.2) as one member of staff noted: “The staff do have the capability for looking at what actually is being viewed on the screen but that is only when we’re given reason to do it otherwise it’s not something that’s used”. The legitimacy of monitoring by staff was not without concerns: “Now as to how widely used that is, I don’t think it is and the ethical implications of that are a grey area as far as I’m concerned because I don’t think it actually notifies the user that they are being monitored, whereas we have software on the corporate side which does that but you do need permission from the actual users for it to occur”.

Some staff expressed concern about the images they sometimes observed that were displayed on the social networking site, Facebook, as one library assistant explained: “Men in here looking at young boys in obscene poses with their trousers and their pants just showing a little bit you know and girls then, with vibrators, posing on Facebook, by their mouths”. She observed this kind of behaviour on a daily basis: “You can see girls posing with their G-strings or sexy clothes, I’d say, almost every day”. Another member of staff detailed a recent incident involving unsuitable images on Facebook: “I had somebody the other day who said ‘that guy’s looking at something, he’s got penises on his screen’ so when I looked he was on Facebook and he was enlarging some of the page photos”. However, it was suggested by one interviewee that if the service tried to block Facebook there would be uproar and that Facebook itself needed to resolve these issues.

One library assistant detailed an incident where she had refused to print off a picture for a user because she found it offensive and had enlisted the help of a colleague who had not: “They only wanted a tattoo, picture of the tattoo but the whole picture itself wasn’t very nice so I refused to do it and got someone else and she did it but she didn’t find it offending, I did. Because he was full frontal”.

**Staff**

To provide Internet access supervisors log the machines on and get them ready for use by the public. Library assistants help users log on to the PCs and retrieve print outs. They also help with basic guidance such as locating a website: “We all take part in logging people on and we’re allowed to help up to a certain point but not too much than just log on to a website and give a little bit of advice”. Staff troubleshoot, for example, when users experience printing problems.

Staff received NOF ICT training in the form of the ECDL from 2002 onwards but identified immediate training needs in order to support users effectively since there was a demonstrable shift in users wanting to access Universal Jobmatch; the government website for job search:

“We now have people coming in because the Job Centres have gone, so they’re coming to do their job searches”.

“All the staff did an ECDL course years ago...but we haven’t had any guidance/teaching to help manage the public”.
Training is usually done in-house but at the time of the case study visit there was a moratorium on training. Staff tend to pick things up by showing users and learning ‘on the job’: “I’ve had to learn myself. Teach myself, sorry”.

Future
Staff felt that there was still demand for the Internet in their libraries and into the future it was anticipated demand might grow especially amongst those unable to afford Internet access at home: “Definitely. I do and it’s growing all the time and I think that as the cost of electricity and things goes up people will be wanting to come here won’t they? They won’t be able to use their own”.

The service is currently waiting for the roll out of WiFi which will also be filtered. The infrastructure is already in place in Merthyr Tydfil Central Library and some handheld devices have been purchased:

“I think the access points are already in place but it still needs to go live and I think the network team are working on that at the moment”.

“We’ve actually bought some tablets, we’ve bought laptops that library users will be able to use with the WiFi and at the moment we can’t use them”.

Good practice
The AUP is detailed and comprehensive and gives staff an effective tool with which to deal with any misuse which is identified. The filtering software is not infallible but staff perceive that it is effective although the new software appears to be in need of some ‘fine tuning’.

Users

User 1
Female, aged between 20 and 34. User 1 is a part time student and comes to the library every day to access the Internet. She also has access at college. User 1 has been using the Internet on the library PCs for the last two years. When using the library PCs she tends to search for jobs, check emails and Facebook. When asked about filtering she wasn’t surprised to learn that the library service used it because “loads of things are blocked”. She finds numerous legitimate sites are blocked including online job applications and assessments but she didn’t think it was worth asking staff to help since “I’ve heard other people ask and I don’t think they can really do anything so I haven’t bothered”.

User 2
Aged between 20 and 34, User 2 is self-employed at present and tends to come to the library three times a week to access the Internet. He tends to manage his workload via his website and advertise for work. Having used the Internet in Merthyr Central Library for the past couple of months he was aware that content was filtered because “some of the websites it will block” but he felt that this seemed to be an arbitrary practice since “it will block a random site where I don’t think there’s any need for it to be blocked”. Although he knew he could ask a member of library staff about a blocked site he wouldn’t ask for a site to be unblocked: “I wouldn’t do it, no, I would just leave it”. User 2 is able to access the Internet on his mobile phone but finds that there are some tasks he prefers to perform on the library PCs.

User 3
Male, aged 20 to 34, not currently in paid employment. User 3 is able to access the Internet from home on his laptop but does not have a mobile phone with Internet access. He comes into the library every day to use the Internet and has been doing so for the last year. His main purpose is to look at
the Universal Jobmatch website but he also reads the news online and watches some video clips on You Tube. User 3 understands how filtering works and is aware it is used in the library. He knows that if he wants a site unblocking he can ask a member of library staff who will contact the IT department but he has never used this process himself to have something unblocked. User 3 feels that the environment in the library is conducive to using the Internet and hopes that in future he will be using it for recreational purposes rather than searching for employment: “I can see myself using it, it’s quieter, you can sit down and do what you need to do and then leave straight away – there are no distractions or anything that you’d have at home or if you were out in the street”.

User 4
Male, aged 20 to 34. Currently employed as an apprentice. User 4 is able to access the Internet at home on a laptop, on a mobile phone and in the library. For the past year he has used the library PCs about twice a week to search for jobs. When questioned about filtering whilst he understands how it works and feels that public libraries ought to filter content he had not realised that online content in Merthyr Tydfil Central Library was filtered even though he had just encountered a site that was blocked in his last PC session. He didn’t think that he would ask library staff about a blocked site: “I just wouldn’t bother to be honest”. User 4 anticipates that he will continue to come to the library to use the Internet until he finds employment.

User 5
Male, age 21. User 5 is in full time work and works nights. He uses the Internet in the library, on his mobile phone and at home on a laptop. He tends to use it in the library twice a week and has been doing so for the last two years. User 5 tends to use the Internet to look at Facebook and search for jobs. He was aware that content was filtered after finding a site blocked in the past and asking a member of staff about it. He is unsure what is blocked but would feel comfortable asking a member of staff about it. In the future he thinks he will continue to come to the library to use the Internet as he prefers to sit at a PC but wasn’t sure he would use the WiFi connection.

User 6
Female, under 20. User 6 is studying part time at a local college. She has access to the Internet in a number of locations including at college, at home and on her mobile phone. She has been coming to the public library for a few months to use the PCs and tends to come to the library once a week to print work off for her college course. User 6 was aware that Internet content in the library was filtered noting that this was the same as the college. The idea of asking staff to unblock a site seemed reasonable and she didn’t feel it would prevent her from using it.
Case Study Data Analysis

This section considers the five case studies as a whole: the qualitative data generated by the case study interviews were analysed using qualitative data analysis (QDA) computer software package, NVivo version 10. The analysis was undertaken with a number of thematic assumptions based on the literature review, the survey results and the five case study visits in which varying members of the MAIPLE team all participated.

The Users

 Were you aware that Internet content in this library is filtered?

Users were almost evenly divided between those that were aware the library filtered Internet content (13) and those that were not (12). Two users did not give an answer.

Of those that were aware, in some instances this was because they had experienced site blocking (3) or because they had noticed it was mentioned in the service’s Acceptable Use Policy/Terms and Conditions (3) or they had assumed it would be (2):

“Yes I just tried to access something, it had a picture of a gun on it so I couldn’t access it but it was actually field sports” (CS2 User 3).

“I’m aware that they must do something like that because there’s a clause that you always agree to go on that, it more or less says that you agree to abide by their policies and procedures and I’d be very surprised in a library didn’t filter the Internet” (CS1 User 3).

“I think it maybe says it on the home... you know, when you log onto the Internet... I think it says” (CS3 User 3).

“Just assumed it was filtered for safety” (CS4 User 3).

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

“It is? So there are things that they just don’t let you on?” (CS2 User 2).

“I had no idea” (CS3 User 1).

“No. I’m not aware at all” (CS5 User 4).

Interestingly one user was surprised to learn that content was filtered because he had noticed other users looking at inappropriate content or ‘under blocking’:

“I didn’t think it was because of some of the sites people can get on” (CS1 User 2).

 Have you ever found a website blocked?

Nine users spoke of their experiences of encountering blocked material online which they perceived to be ‘over blocking’:

“Just a dating website but it’s for over 18s. It’s not like pornography or anything but it wouldn’t let me on it. I thought it was down. And going on YouTube, I wanted to watch Saddam Hussein get hung but it wouldn’t let me” (CS1 User 1).
“I was looking up something... something just anonymous like but it just come up ‘this site is blocked’ and I asked the girl at the desk and she said she didn’t know why because it was innocent” (CS4 User 3).

“No because some things are blocked totally. I’ve been on the web looking for jobs and they are blocking things that are just totally legitimate and there’s nothing, no reason that they should block them. Not everything. Obviously porn and stuff, I think that’s fine, just not everything they should block” (CS5 User 1).

“Sometimes it will block a random site where I don’t think there’s any need for it to be blocked” (CS5 User 2).

Comments from users suggest that there was some confusion about the kinds of content that the various library services did block:

“I don’t know exactly what is blocked” (CS3 User 2).

“Don’t know what they do block” (CS 5 User 5).

“Not aware of how or why certain things are blocked” (CS6 User 6).

Would you feel comfortable asking staff to unblock a legitimate site for you?

Of the 21 users that responded to this question, 11 said that they would feel comfortable approaching staff whilst ten said they would not:

“I think I’d just ask a librarian because if they don’t know they tend to say they’ll ask this other librarian” (CS3 User 3).

“It wouldn’t bother me” (CS5 User 6).

Most of the users who felt that asking staff was not an option for them tended to focus on how asking staff might make them feel or how staff might perceive them; “shady” (CS1 User 2); “embarrassing” (CS2 User 1); “concerned” (CS3 User 1); “awkward” (CS4 User 6) while a couple of users in one particular case study site felt that staff were unable to help them even if they did ask:

“I just don’t think they can do much so I wouldn’t bother” (CS5 User 1).

“I just wouldn’t bother to be honest” (CS5 User 4).

Should public libraries filter Internet content?

Nineteen users were pro-filtering and eight were unsure. Two users were definite ‘no’s’. Users in agreement with the use of filtering tended to agree that it was appropriate for a number of reasons including the presence of children in public libraries, in order for libraries to maintain standards of public decency and to ensure libraries only provide access to content which is permitted by law:

“Adult ones, 18 and that? Yes, it should yes. You don’t come to the library to look at porn and stuff like that do you? Sit there at the table cracking one off. Plus kids can go on it can’t they? Yes, it should be blocked, definitely” (CS1 User 1).

“Oh aye, definitely. Especially for kids’ sakes, children’s sakes” (CS4 User 1).

“I think they should filter as the Internet is used by everybody” (CS3 User 4).
“I’d say so, I think in the same way you wouldn’t have certain material on the bookshelves, I don’t see why you wouldn’t apply the same idea to Internet access. I mean it’s a public service and I think there are certain restrictions which you would consider decent” (CS1 User 4).

“Definitely. Because some things are legal to look at and some things are not and with the Internet being international and things can come from other countries and so on” (CS3 User 3).

“Yes because when you think about it there are some things on the Internet that shouldn’t be on the Internet in the first place and you don’t want the libraries getting into trouble” (CS5 User 3).

The Staff
Of the 31 staff analysed here, 15 interact regularly with the public while 16 do so irregularly, if at all. In terms of level within their organisations, 15 are frontline staff, 13 are middle managers and three are senior staff.

Is it ethical to filter Internet content in public libraries?
Twenty two staff felt that it was ethical to use filtering software in public libraries whilst nine expressed some hesitancy or regret. When staff responded to this question, for some, it was very clear that filtering was an obvious tool to implement in this environment whilst some spoke in terms of it being a pragmatic means to an end when providing a service to a diverse range of people:

“I think inevitably when you are dealing with a whole community; you have to start thinking about if somebody was looking at a site which would be very offensive to another member of the community. I think you can’t just avoid the fact... Total freedom on the Internet I think is a wonderful idea, like total freedom everywhere but if society is going to work I think there’s bound to be, there has to be some restrictions” (CS2 Library Advisor 1).

“Absolutely. Absolutely. People cannot be trusted – simple as that” (CS2 Library Advisor 3).

“I don’t think there is any ethical implication... We’re just trying to prevent sites from being accessed that could cause offence to other people” (CS3 ICT Manager).

“In a public place I do think it’s ethical. It might be discriminating against people but I don’t think it is” (CS4 Library Assistant).

Staff expressing some reservation about filtering spoke in terms of it being a “challenge” (CS1 Assistant Director); “unfortunately” (CS2 Senior Manager); “difficult” (CS2 Team Leader 1); “regretfully” (CS3 Head of Libraries); “double standard” (CS4 Operational Manager); “sensitive area” (CS5 Desktop Services Engineer) and “ideally” (CS5 Operations Librarian).

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

“We did think long and hard about it because in many ways filtering is anathema to librarians” (CS1 Assistant Director).

“We’ve a double standard because we say we’re fiercely proud of the fact that we don’t censor, that we don’t censor the published word unless it is something that we’re not permitted to carry but we will censor the visual and it’s the visual which is the problem” (CS4 Operational Manager).
The justification for its employment was the protection of children and young people (eight staff) and appropriateness in a public space (seven staff):

“Especially when you have got young children coming in without their parents” (CS1 Library Assistant)

“I can have an eight year old child sat next to somebody. There needs to be some filtering to protect those people” (CS5 Operations Librarian).

“What people do in their own homes is fine but in a public place there needs to be some control I think because as I say our PCs are visible to anybody here sitting out there watching something” (CS4 Branch Library Manager 1).

Terms used in relation to the public nature of library space included “insurance” (CS1 Senior Librarian) and “protect” (CS4 Branch Library Manager 2), “trust” (CS2 Library Advisor) and “safe” (CS2 Team Leader 2).

All five case study services use filtering software. However, we did ask staff about unacceptable use of the Internet in spite of the presence of filtering. Twenty six staff recalled misuse incidents they had witnessed whilst in post. They tended to be users viewing material such as pornography although sites containing images of child abuse, necrophilia and terrorist content were also mentioned as well as copyright infringements or file sharing. The perception overall was that misuse did take place but it was not an overwhelming problem and had diminished over time since the Internet was first introduced:

“It’s only the odd person but if an odd person is upsetting other people around them, then it causes a problem” (CS1 Senior Librarian).

“We have had issues around people trying to access certain sites and some of the sites that they’ve accessed have been quite inappropriate especially when you’re sitting in a public building and you might be sat quite close to someone else. We’ve had complaints from the public because somebody’s may be accessed pornography or, even worse, necrophilia sites, things like that or you know, we’ve had issues around terrorist sites as well” (CS3 Community Engagement Manager).

“We’ve had a few incidents where people have been on porn sites, different sites that are not suitable for library use and it is usually me that ends up going and giving them an earful” (CS5 Member Support).

One case study site had recently caught and banned a user who had been illegally downloading films in the library:

“The person who done it sat in a crafty position because we couldn’t see him and he had a USB stick and even IT said ‘how’d he done it?’ Because he’d managed to override the security system and he was there for two or three hours and we didn’t realise then he was downloading films” (CS5 Assistant Librarian).

“I have recently banned a gentleman for doing it. I informed IT at the time because he was downloading them for commercial use and I caught him and we followed the history of what he had been downloading and when he came back to use the computers later on, I told him he was banned” (CS5 Member Support).
However, whilst frontline staff were not always sure about file sharing, uploading or downloading, a senior manager or member of the ICT team interviewed usually was:

“We don’t allow people the freedom to install their own software onto PCs so the capacity to engage in file-sharing for instance is severely curtailed… we don’t allow breaches of copyright law on computers” (CS1 Service Relationship Manager).

“We don’t allow file-sharing on the network. Copyright is a much tougher one... So file-sharing is blocked out now and has been for quite a while but that was partly driven by network capacity issues as much as potential for piracy and the transmission of what we call content which we could normally block out” (CS2 Senior Manager).

“We don’t allow file-sharing for instance is severely curtailed… we don’t allow breaches of copyright law on computers” (CS1 Service Relationship Manager).

“We don’t allow file-sharing on the network. Copyright is a much tougher one... So file-sharing is blocked out now and has been for quite a while but that was partly driven by network capacity issues as much as potential for piracy and the transmission of what we call content which we could normally block out” (CS2 Senior Manager).

“With file sharing, peer to peer, all that sort of stuff, I’d say we’re fairly tight. I’m not saying we’re 100 per cent perfect because somebody will always find a way to get through but once we see a breach to the network we’ll go and deal with it and lock it down” (CS4 Project and Service Manager).

“The ports that would enable things like torrents and specifically file sharing applications are blocked through the network so they wouldn’t be able to use that sort of angle” (CS5 Desktop Services Engineer).

Do you ever get any complaints from users about filtering?
Twenty-three staff spoke about their experiences of ‘over blocking’. It wasn’t perceived to be a major problem but it did happen. Often it was innocuous, where a seemingly legitimate site was blocked but a couple of staff spoke about instances that were a little more complicated:

“It’s not a recent issue. It’s the one that sticks in my mind. We had a local candidate for the British National Party and it may well have been this library that he used. He complained to us that he couldn’t access the website of his own political organisation. Again, ethically, whatever you think about it, it’s not a banned organisation in the U.K... It’s a legally available organisation... There are no proscribed actions to be taken against the BNP. So that was freed up” (CS1 Assistant Director).

“We have had complaints in the past from people who have said that we’re sort of casting value judgments on, let’s say for example, their sexuality and we’ve been at pains to point out, I’m thinking of a specific complaint here, we’re not filtering... he was homosexual, we’re not filtering gay sites but if it’s a gay porn site, yes, we’ll filter that” (CS4 Operational Manager).

In one particular case study site, a change in the filtering software seemed to have triggered a wave of sites being blocked:

“There was one gentleman who said he listens to military music. Well they stopped that site. Well I phone up IT to ask them and they said, ‘well what it is, due to our new filter system, there’s certain sites that can’t be accessed’ and they said there is nothing we can do about it” (CS5 Assistant Librarian).

“We’ve got a gentleman who was trying to find WW1 and WW2 websites and because it was weapons, it was blocked and that can be very frustrating because it’s something that is quite legitimate, looking up for archive history” (CS5 Member Support).

“They brought the new one in and suddenly sites that people had been accessing like the Royal Artillery site where somebody’s doing family history research and they’re looking at the museum and that was suddenly blocked because it was artillery, it was weapons” (CS5 Operations Librarian).
Five members of staff voiced their experiences of users experiencing ‘under blocking’ most of which involved users viewing pornographic sites:

“There was one incident where one gentleman was always coming in and choosing the back one [PC]. One of the security guys noticed that he was accessing porn sites” (CS3 Community Engagement Manager).

“We’ve had a few incidents where people have been on porn sites, different sites that are not suitable for library use... What they use at home and what they have here are different, we’re not talking child porn sites, we are just talking general porn and it’s not suitable to see that on a screen in the library” (CS5 Member Support).

“You’d get the odd one where they’ve been looking at pictures of other... revealing pictures of... as I say the YouTube video or whatever” (CS2 Team Leader).

Getting sites unblocked?
Staff in the five case study services are able to request that sites are unblocked for users which in four services involves liaison with IT colleagues:

“We would have to phone up our IT support and say to them ‘could you unblock this website for us?’ Because we wouldn’t consider it to be unsuitable” (CS2 Team Leader).

“To be honest, I have to say that it’s quite ad-hoc. It’s generally brought up through me and I then take it through to the IT team who then would unblock it for me” (CS3 Head of Libraries).

“Well it comes up Administrator and they [IT] are the only ones that can... we can’t... and they said ‘that’s it, if that comes up then you can’t get on that site’. So you explain it to the customer and he said ‘well, it’s a universal site’ and we said ‘yes but there’s nothing we can do about it’. You try to explain to them and most of them say ‘Alright, fair enough’ but that’s the way it is” (CS5 Assistant Librarian).

Do staff receive any training or support in relation to supporting Internet users?
Staff who had been in post for at least a decade referred to the training provided as part of the New Opportunities Fund ICT Training for Public Library Staff which in many cases was the European Computer Driving Licence (ECDL):

“I know it’s going back a bit but when we introduced People’s Network obviously a lot of staff did European Computer Driving Licence (ECDL) and a lot of those staff are still with us” (CS1 Assistant Director).

“I did ECDL a few years ago. I’m not quite sure how much help that actually was in a way but anyway I’ve done that but other than that there’s not been an awful lot of training” (CS2 Library Advisor 2).

“I know we did ECDL about 12 years ago but that was just the basics” (CS4 Branch Library Manager 2).

“All the staff did an ECDL course years ago but that was just for people to familiarise themselves with things like word processing and making things bigger” (CS5 Library Assistant 2).
Staff tended to receive training when new software was introduced such as a new booking system but the overwhelming message was that training was almost non-existent and staff had to simply acquire skills 'on the job':

“We get some in-house training sessions here particularly when things change like with the self-service – NetLoan we call it and when our databases are updated the Librarian will sometimes have a few of us together and we’ll just have a look at it and we’ll see what’s available. But the rest of it is really what you pick up as you go along and I think a lot of us are self-taught really and I think you’re sometimes embarrassed that the customer know more than you do, I mean, there are some real experts out there” (CS1 Assistant Library Manager).

“When we had our new Library Management System obviously everybody had training but a lot of... it’s kind of, on-the-job really” (CS3 Community Engagement Manager).

“We did have very, very basic training when they introduced Windows 10 [sic] but basically it’s on-the-job learning” (CS4 Branch Library Manager).

**Is visual monitoring a useful way to manage acceptable Internet use?**

Staff monitoring what was being viewed on the PCs by walking around the building was seen by some staff as a useful, if sometimes limited way, to ensure acceptable use:

“The physical layout of the PCs is quite important because that, we could say, is using peer group pressure in a sense as well as staff and that’s good up to a point” (CS2 Senior Manager).

“Where possible I’d say staff are very good just because they’re out and about and sort of around their branch area. They know their customers, they know their regulars, they know somebody who’s only ‘they’re in, they’re out’. Certainly in the majority of our libraries where possible we would have adults and children separated... But I wouldn’t like the responsibility to be on staff alone without proper software in place. It wouldn’t work” (CS4 Project and Service Manager).

“We do check. I know I go in every ten to fifteen minutes and check what’s going on in there [PC Room]. That’s from personal paranoia because I know that a lot of them that we get tend to sort of congregate in groups around one computer and that, again, is not acceptable because they are overlooking what somebody next to them is doing and it could be personal information” (CS5 Member Support).

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

“The system that we use here at the moment is a system called iCam, like a cyber café management software. It will enable the staff member to actually shadow the screen” (CS5 Desktop Services Engineer).

“If somebody came in and they said to somebody on the desk ‘that guy over there’s looking at something’ or whatever then the staff do have the capability for looking at what actually is being viewed on the screen but that is only when we’re given reason to do it” (CS5 Operations Librarian).

A small number of staff were dismissive of visual monitoring because they did not have the time to do it:
“We have that many other things to do nowadays it’s not as if we can sit there just waiting for the next thing to... ‘Oh I’ll just keep an eye on that’” (CS2 Library Advisor 3).

“We have tried to monitor it because they have memory sticks which they can plug in but you can’t stand over their shoulder” (CS3 Site Support Officer).

**Demand for WiFi?**

At the time of the case study research not all the sites had wireless Internet access for the public. Of the three that did (CS1, CS2 and CS3), staff perceived that it had been well received:

“A lot of people do come in to use WiFi, Bluetooth etc.” (CS1 Access and Inclusion Librarian).

“It’s been so successful. When you walk round the library you’ll see people on their laptops everywhere including down in the coffee bar here because we’ve got a point down here” (CS1 Senior Librarian).

“There’s a lot of laptop use and a lot of tablet use and people using phones as well, using the Internet through their phone through the WiFi” (CS2 Library Advisor 4).

“I think since we put the WiFi in the number of people sitting here with their own equipment is significant, very significant, to the extent whereby we think that we need to reorganise the layout of the building to deal with it” (CS3 Head of Libraries).

Case study sites 4 and 5 were waiting for WiFi at the time of the fieldwork. They anticipated it would be widely used:

“Personally I think it’ll be more than the people who come in to use our computers because that’s what people expect now” (CS4 Project Officer).

“I should think so, yes, because we’ve had quite a number of people coming asking if we’ve got WiFi and we have got it, it’s just not set up. I think it will be popular” (CS5 Library Assistant 2).

**Popularity in accessing government services online**

An issue which emerged during the interviews but which was not explicitly explored was that of users accessing government services including the Universal Jobmatch website and applying for benefits online. Sixteen staff and twelve users spoke about job searching. Staff had observed that users were increasingly searching for jobs and applying for benefits online some of whom had been directed by Job Centre personnel to use the Internet in the library:

“A lot have been sent through from the Job Centre because I think a lot have been taken... a lot of the application forms for things like housing it’s all done online. When people say ‘I don’t know how to do that, I haven’t got a computer’, the Job Centres are saying ‘Go to your library, they can help you’” (CS3 Library Officer).

“We do have people you know... expectations. ‘We’ve come here; Job Centre’s sent me to do my CV’” (CS3 Site Support Officer).

“Just the Job Centre directed me to come over to use the library as a resource to help me with any researches or applications online” (CS3 User 1).
This appeared to be an issue in Case Study site 3 in particular but was also echoed in Case Study site 5:

“The Job Centre sends them here so that they can do their job search and complete... they have to apply for X number of jobs or go on the web to find jobs so many days a week otherwise their benefits are cut and we do see people who are awfully worried by this and some people have had their benefits cut” (CS5 Member Support).

“A vast majority are computer literate but there’s an awful lot not and the Job Centre sends them over and they haven’t got a clue how to use a computer or a keyboard. So we are involved with all that, putting them on the [Universal] Job [Site] UK and that, so it’s a lot of work” (CS5 Library Assistant 2).

“I usually use it mainly to look for jobs on Universal Jobmatch and any other job sites” (CS5 User 3).

There were comments to suggest that some of these users needed a lot of support which staff were not always able to provide given the constraints of time or that they did not feel suitably skilled to help with:

“But we still do get a lot of people that don’t have Internet at home and something in their lives has come along... and they are coming in and they have never used a computer before” (CS2 Library Advisor 3).

“We can certainly help them get online but we haven’t got the facilities and staff to actually sit down and go through a housing benefit form or something like that. The same thing for job applications” (CS3 Library Officer).

“We have had people come in wanting to do computer training because they’re looking for a job as a cleaner but the application is online and they haven’t a clue” (CS4 Branch Library Manager 1).

“We’re only supposed to get them on [line] but not being disrespectful to some people, they are not very computer literate so with the Government now using Universal Job Search and also the doctors sending them down to self-certify, we spend more time on computers now to help people. We can’t just leave then because they say ‘Well how do I get on Universal Job Search?’” (CS5 Assistant Librarian).
Public WiFi in the UK: Desk Research

This section considers the approaches used by commercial Internet providers in providing WiFi to customers as a base for comparison with public libraries in the UK. It explores their adoption of technical measures such as filtering software and organisational measures such as AUPs or Terms and Conditions in managing acceptable WiFi use. The findings detailed here are based on a thorough search of the literature available in the public domain on the Internet and in academic journals in relation to commercial outlets providing WiFi. A number of well-known commercial outlets a user might reasonably come across in a UK city were researched. In addition, the ease of locating any AUP or Terms and Conditions on a company’s website was also explored.

Public WiFi in the UK

The UK Council for Child Internet Safety (UKCCIS) is a group of more than 200 organisations working in partnership to help keep children safe online. The first meeting of the UKCCIS Board was held in early 2012 and included MPs and representatives from industry and relevant charities working in the field. The public WiFi strand has been led by Anne Heal from BT Openzone since July 2012. In the minutes of that board meeting three main areas of broadband were mentioned that the public WiFi project would include – retail, public places including "libraries" and private/public WiFi access (p.4). By February 2013, Ms. Heal reported that progress had been made with the six largest public WiFi providers "who together account for upwards of 96 per cent of public WiFi provision" (p.5) in what they could do to filter adult content and by May of the same year "All providers now either filter by default or offer business customers the choice to filter" (p.5). In the summer of 2013, the Department for Culture, Media and Sport announced at a summit on tackling child sexual abuse online, that the main public WiFi providers had pledged to offer family-friendly WiFi "in public places where children are likely to be" (DCMS, 2013). This was to have been completed by the end of August 2013 according to an article in PCMag.com: "An agreement was also reached with O2, Virgin Media, Sky, Nomad, BT and Arqiva to apply the automatic family filters to public WiFi access points by the end of August" (Strange, 2013). According to UKCCIS Board notes from July 2013, "the WiFi work only filters pornography".

Media stories (Gibbs, 2013) published in November 2013 based on an initial story published in the Daily Mirror newspaper suggested progress was patchy: “But a test of 129 free wifi hotspots around the UK including shops, cafes and children’s play areas has found that 32 of them did not block access to pornhub.com, a free website that streams hardcore pornographic videos" (Wales Online, 2013).

The original investigation into public WiFi was undertaken by Adaptive Mobile and the publication Courting trouble: why WIFI hotspots need to be part of the safety debate (Adaptive Mobile, 2013) reports research using mystery shoppers who looked at WiFi hotspots in a number of cities in the UK (London, Birmingham and Manchester) and in the U.S.A. (New York, Boston and San Francisco). Locations included cafes, hotels, shops, restaurants and public spaces including libraries and train stations totalling 179 in the UK and 86 in the U.S.A. In the UK, public space hotspots were “the most aggressive blockers of content but still nearly 1 in 10 allowed access to pornography” (p.9) and were also the locations where over blocking was most likely to occur: “Half of all retail and public space WiFi hotspots blocked access to a hidden word site, compared with only two in every 10 cafes and restaurants and one in 10 hotels” (p.12).

In comparison, in the U.S.A. the researchers found little WiFi filtering: “the US researchers found no blocking at all of any types of potentially harmful or offensive content in any cafes, and very little blocking of any content in restaurants” (p.13).
A recent report by providers of wireless hotspot software, Purple WiFi, which attracted responses from more than 3,500 respondents across more than 40 countries, found that the majority of businesses including hoteliers and retailers offered WiFi to users with three quarters of them providing it free of charge. In relation to content, 41 per cent had filtering in place, 33 per cent did not and 26 per cent did not know.

The top six public WiFi providers

1. **O2**
   
   O2 Wifi is used by brands such as Costa Coffee, Debenhams, McDonalds, Tesco, Subway and Pizza Hut.

   O2 Wifi is subject to content filtering and according to O2 has filtered since its inception “From the moment our public wifi service was switched on in 2011, we’ve fully content-filtered our service at all venues” claiming to be the first in the industry to do so (O2, 2013).

   The O2 Wifi Terms of Service are available on the O2 website. It notes in ‘The Service and what you can expect from us’ that “The service may be subject to content filters which either prohibit or require age verification to access content on the Internet which we may classify is suitable for over 18s only. We will use our discretion to determine what is or isn’t adult content”. If a user does not agree with the classification of a particular site they are able to contact O2 by email “to raise concerns” but ultimately “if you don’t agree with our classification then you are free to stop using the service at any time” (O2 Wifi 2014, p.1).

   ‘What you must not do’ comprises using the WiFi for “unlawful, fraudulent, criminal or otherwise illegal activities” (p.3) which includes uploading and/or downloading material which is offensive, obscene or unlawful or breaches copyright or intellectual property.

2. **Virgin Media**

   Virgin Media WiFi is available on the London Underground. The Virgin Media WiFi site’s FAQs refer to its Terms and Conditions which “vary depending on which provider you connect with” providing links to Virgin Media, EE, Vodafone, O2 and Virgin Media WiFi Pass. The Virgin Media link directs you to a list of ‘legal stuff’ which includes its Acceptable Use Policy. There is no mention of filtering within this AUP which appears to relate to use of Internet services in general. It does however state clearly that “You must not use our services in any way that is unlawful or illegal or in any way to the detriment of other Internet users” (3.1) and “you agree to comply with (and ensure that others using the services comply with) all applicable laws, statutes and regulations in connection with the services” (3.2).

   Filtering is referred to indirectly in the FAQs; ‘Does Virgin Media block any content on WiFi on the London Underground?’ - “As WiFi on the London Underground is a public WiFi network, Virgin Media has a responsibility to ensure that the content available is suitable for young people to access themselves or to look at over someone else’s shoulder” (Virgin Media, 2012).

3. **Sky**

   A BskyB product, The Cloud WiFi is used by brands such as Pizza Express, M&S, WH Smith, Cafe Nero, Network Rail and Wetherspoon pubs.

   The Cloud WiFi is filtered by default and companies may opt-out if they wish. Categories blocked by default are violence, hate and racism, pornography, illegal drugs, hacking and proxy avoidance, criminal and illegal skills, nudity.
There is an Acceptable Use Policy and “By pressing that continue button on the registration page you are indicating that you agree to the terms and conditions of the Contract” (p.1). Interestingly, section 4.5 states: “You agree to indemnify us against all losses, liabilities, costs (including legal costs) and expenses which may incur as a result of third party claims against us arising from, or in connection with, your misuse of the WiFi Service or breach of this Contract” (p.2). Page 4 of the AUP goes into detail on what it calls its ‘Network Management Policy’ which is where information is provided about blocking. It notes that it relies on URLs provided by the Internet Watch Foundation as well as URLs relating to drug use, pornography, offensive or illegal speech, and network malfeasance. They request that WiFi users “Don’t use the WiFi Service illegally!” (p.4) and ask that users do not use the WiFi service to “send, receive, store, distribute, transmit, post, upload or download any materials or data which” violates any law, is defamatory or harmful to minors amongst other stipulations.

According to The Cloud website page on staying safe online, filtering categories are “compiled by a 3rd party company and may be subject to change”. The AUP directs users to a website to check on the status of individual sites which may be blocked which is a SonicWALL page. SonicWALL produce Internet content control appliances and was acquired by Dell in 2012.

A case study of Pizza Express’s experience of using The Cloud since 2011 across its 400 restaurants notes: “The Cloud ensures that every restaurant is provided with a safe browsing experience, filtering out adult sites that are unsuitable for a family restaurant” (The Cloud, nd).

4. Nomad
Nomad Digital is a provider of wireless solutions to the transportation industry and customers in the UK include East Midlands Trains Meridian fleet and Virgin Trains (Nomad Digital Ltd, 2013). It is not clear whether Nomad provide filtered Internet content to their UK customers. According to East Midlands Trains’ WiFi Terms and Conditions available on the East Midlands Trains website, they ask that users do not “use the service for anything unlawful, immoral or improper” (3.1a), “you do not use the service to harm or attempt to harm minors in any way” (3.1c) and “the service is used in accordance with any third party policies for acceptable use or any relevant Internet standards (where applicable)” (3.1g). There is no mention of filtering but there is a content disclaimer which advises “East Midlands Trains does not control, nor is it in any way liable for, data or content that you access or receive via the service. The Internet contains unedited materials, some of which are sexually explicit or may be offensive to you. East Midlands Trains has no control over and accepts no responsibility for such materials” (4.1).

Virgin Trains WiFi FAQs do not refer to filtering rather they urge users “that as you are sitting in a public environment, please do not view content that others may find offensive or inappropriate” and to note that access to some sites is restricted on the grounds that they may breach copyright “to comply with the Digital Economy Act 2010 and to ensure the best possible service quality for all customers of the WiFi service, we reserve the right to restrict access to certain websites that may be deemed to potentially infringe copyright” (Virgin Trains, 2014).

5. BT
BT WiFi formerly known as BT Openzone is used by brands such as John Lewis, Starbucks, Fenwick and Burger King. BT WiFi is unusual in that it offers its customers or partners the opportunity to restrict access but filtering is not a default option or a feature which is promoted over another. BT offer Bt WiFi Protect which conforms with the public WiFi initiative in the UK allowing “our WiFi partners to restrict access to pornographic websites”. Emphasised as a
benefit, this product “allows BT WiFi site partners who choose to apply content filtering, to block access to pornographic material” (BT wifi, nd).

BT WiFi Acceptable Use Policy (including BT Openzone) details prohibited uses which include illegal/criminal activity such as “theft or infringement of copyrights, patents, trademarks, trade secrets, or other intellectual property”; security violations; threats; offensive materials – “The BT Network may not be used to transmit or store material of an offensive nature, including obscene, pornographic, indecent, abusive and harmful materials, or to transmit to recipients material which is inappropriate for them, including obscene or offensive materials to children” or spam. If BT detect a violation of their policy they may take action, however, they attempt to reassure the user that “it is not our intent to monitor, control, or censor communications on the BT Network”. Interestingly, filtering may be used in response to a violation: “Violations of this Policy may result in a demand for immediate removal of offending material, immediate temporary or permanent filtering, blocked access, suspension or termination of service, or other response appropriate to the violation, as we determine in our discretion” (BT wifi Terms and Conditions, nd).

In 2009, Starbucks began offering BT Openzone WiFi in their coffee shops, free to those with a Starbucks reward scheme card. In 2011, this qualifier was removed and Starbucks rolled out free BT Wifi in all of its UK stores. Users have to accept the terms and conditions of using the Wifi on a pop up. Starbucks was the subject of some controversial media coverage in 2012 when it was revealed that customers were able to view pornographic material. John Carr, an Internet safety expert and secretary of the Children’s Charities Coalition on Internet Safety, discovered that WiFi in Starbucks was unfiltered. Following a number of failed lines of conversation with Starbucks he briefed a member of the House of Lords and it was mentioned in a debate on online child protection in Parliament and picked up by a number of media outlets. In 2013, Starbucks moved to filter pornographic content. The Starbucks website does not mention filtering or acceptable use. It refers to BT Openzone as its WiFi provider and provides a link to their site.

BT are working with Mumsnet as part of the Family Friendly WiFi programme. Mumsnet writes “We will also be working with BT, the UK’s biggest provider of public WiFi through BT Openzone, to research the concerns parents have about their families accessing content on the move and inform BT’s WiFi strategy” (Mumsnet, 2012).

6. Arqiva
Formerly known as Spectrum Interactive, Arqiva WiFi is used by the Whitbread restaurant brand, Brewers Fayre. The Terms & Conditions Acceptable Use Policy available on the Arqiva website which includes WiFi, details prohibited uses including storing, sending or distributing copyright materials, anything unlawful or illegal or which may offend. If a breach of policy occurs, Arqiva may issue a warning to the user, withdraw its services, start legal proceedings or disclose information to law enforcement authorities. There is also a Terms & Conditions and Privacy policy for WiFi services which must be read before using the WiFi service. There is no mention of filtering within either of these Terms and Conditions documents. However, filtering is detailed in relation to Internet kiosks which can be found in hotels and airports: “This Kiosk includes several website filtering packages. Sites blocked include those deemed by Arqiva and its partners to be inappropriate. However by accepting these Terms and Conditions, you agree that it is not possible to successfully block 100% of inappropriate content. If this is a concern, please do not use this Kiosk. Specific sites can be unblocked by writing to wifisupport@arqiva.com. (The process takes two working days)” (Arqiva, nd). Heathrow Airport which uses Arqiva WiFi is very clear that the service is filtered, highlighting its family friendly credentials in the WiFi FAQs on its
website. According to the website, thinkbroadband.com who contacted Arqiva in June 2013, “apply content filtering in accordance with the clients’ requirements. Where no requirements are specified by the client, we implement ‘family-friendly’ content filtering as a default” (Ferguson, 2013).

A summary table mapping the use and provider of filtering software in a range of commercial outlets is provided in Appendix 3.
Workshop

To complement the other strands of the research strategy, a one-day workshop was held at Loughborough University on 10th July 2014. The purpose of the workshop was to further test the reliability and validity of the project findings, as well as to disseminate them to practitioners and policy makers and engage with other relevant stakeholders. The methods used to gain feedback on the findings included presentation of findings followed by public discussion; break-out groups to explore specific issues in greater depth; and a panel discussion chaired by a member of the stakeholder community. The panel debated questions from the audience related to the project findings. The recommendations from the project were included in this discussion. In summary, the project recommendations were broadly endorsed; in particular, the notion that it is unrealistic to bypass filtering as one solution in the ‘acceptable use’ toolbox was generally accepted, with the caveat that there was also a need for greater transparency and more attention paid to training and education of both staff and users. A full report from the workshop can be found in Appendix 2.
DISCUSSION
This research project has addressed the gap in knowledge with regard to the measures currently being taken by UK Public Library Services to manage and regulate public access to Internet content. In doing so, it has revealed that filtering software is an apparently ubiquitous solution in place to control and protect access to ‘inappropriate’, illegal and harmful Internet content. Previous research carried out at the start of the 21st Century (Willson and Oulton, 2000) reported that 71% of UK Public Library Services were using filtering software: the current research suggests that this figure is now closer to 100%. This supports the findings of Brown & McMenemy (2013) with regard to the use of filtering software in Scottish public libraries. However, this general acceptance of filtering software appears to have taken place with little debate or transparency among the profession, and indeed, the decision to filter is led by local authority senior management or local authority IT departments (48.8% of responding authorities, compared with 30% of authorities in which the decision was led by library service senior management or library IT personnel). In devolving decisions on who has access to what content to IT personnel who, rightly, have a primary concern with security of their service, librarians may potentially be leaving the door open to a more conservative and more restrictive level of access to information than would be the case if they themselves were responsible for decision-making in this sensitive arena. In practice, librarians appear in many cases to have been side-stepped in the process (or have chosen not to get involved), and in a few cases, were not able to say whether or not access in their library was filtered. This seemingly passive acceptance of filtering appears to contrast with the position in the US, where there has been strong professional protest at its implementation (Bertot et al, 2010).

It could be suggested that the ‘outsourcing’ of filtering to software companies and/or Internet Service Providers is akin to the outsourcing of book selection to commercial book selection services: however, there is a critical distinction to be made between the ‘selecting in’ of resources, and the withholding of access to otherwise freely available and perfectly lawful information. Of course, in the case of illegal resources, this is a mandatory course of action for public library services. However, when it comes to material deemed ‘inappropriate’ this can be very subjective. Who deems what is inappropriate? In our research, it appears that such decisions have been left primarily to the vendors of filtering software solutions, some of whom have been shown in the past to have distinct ideological biases (Resnick et al., 2004; Radom, 2007). Whilst the current study has not examined any ideological bias evidenced by the suppliers used by UK libraries, our findings do provide clear indications that the inclusion of sites in blocked categories is done in a somewhat unsophisticated way. This ‘withholding of access’ to material can surely be described as censorship by another name, and therefore could be argued to contradict the professional duty and ethic of librarianship to oppose all forms of censorship. Evidence from the findings suggests that, in some instances, librarians are keen to embrace filtering as a pragmatic solution to resolve concerns about possible misuse of computer facilities on the grounds of convenience, expressed in comments such as “We as staff prefer it filtered” (CS4). Examples abounded of users who had tried to access legal and legitimate sites, such as dating websites, job application sites, and military history sites, all of which were blocked. Moreover, many users felt uncomfortable about asking staff to unblock sites, and generally would not do so. Furthermore, in taking decisions to block en masse access to content such as social media to users below the age of 16 (CS5), the public library service risks alienating the very clientele upon whose custom the future survival of that service may rest.

It must be acknowledged that the findings of the research suggest not just widespread implementation of filtering software, but also widespread acceptance of this measure by both library personnel and users alike. The concept of the library as a ‘decent’ public space that is to be trusted as the purveyor of reliable, high quality information (Crook, 1999) appears to outweigh an ethic of
'access to all publicly available information' (CILIP, 2005). Such a debate rests on the fundamental political ideology that underpins the purpose and mission of a public library service – is it to educate, to inform, to offer recreation and a social space, or to improve lives, strengthen communities and reduce social exclusion (Goulding, 2006)? Or, perhaps, it is a combination of all of these.

In addition to the reliance on filtering software, use of public access computers in libraries appears to be a highly monitored – or at least, auditable – activity. Whilst we found that real-time surveillance is mostly limited to visual monitoring of PC screens, the almost ubiquitous use of automated booking systems and individual user IDs for logging onto the Internet ensures that there is the option of checking user history files. Not only does this enable staff to identify the client responsible in the event of a breach of the AUP, it also has the potential to encourage self-censorship on the part of users. Visual monitoring by staff was identified in some instances to pose privacy issues with regard to users who may be displaying personal information – e.g. banking details – on screen, although fewer privacy concerns appeared to be raised with regard to the arguably more intrusive measure of analysing logs of sites visited. There is scope for further research into the privacy implications of monitoring of user web logs in public libraries.

Another method used to ensure safe and ‘appropriate’ use of library IT facilities is the publication of an Acceptable Use Policy (AUP). Although Sturges (2002) has advocated preferred use of the term ‘Internet Use Policy’ on the grounds that the term ‘acceptable’ is inherently subjective, AUP has become firmly established as the preferred term in practice. We found that all except one library declared having an AUP (in some instances, referred to as ‘Terms and Conditions’, or similar title) in place (the remaining service was uncertain as to whether one existed). There is much guidance available as to the recommended content of an AUP (see for example Sturges, 2002 and McMenemy, 2014), so our recommendations do not focus specifically on this aspect. But it is clear from our findings that having such a policy in place is necessary from the perspective of protection of the service itself in the event of serious misuse of facilities, and as guidance to users as to the purpose and scope of the service provided, as well as to what constitutes ‘acceptable’ use on their part. However, what was found to be lacking was general awareness of the policy on the part of users, and in some cases, also on the part of staff. Much more attention needs to be paid to promotion and awareness-raising with regard to the AUP, and concomitant training of personnel. The presentation of such policies is also worthy of attention: for example, are they written in an accessible style and visually presented in an eye-catching and user-friendly design, using graphic means such as icons to help users navigate and understand the content?

At the time when the case study field work was conducted (2013-14), the need to avoid Intellectual Property Rights infringement and the anticipated potential impact of the Digital Economy Act were also found to be informing approaches to the regulation of Internet access. Senior personnel at the case study sites appeared to have good understanding of the implications and complications that the Act might entail for library services, and the legal obligations that it could impose. However, on the ground, it seems that library personnel are less well briefed with regard to copyright issues in the digital environment. Evidence from the findings suggested that, not only are library personnel not fully safeguarding against copyright infringement, but they do not always identify it when it occurs. This is again an area ripe for further training to be offered.

6 Sections 17 and 18 of the Act would have allowed copyright holders to apply to a court to secure a website blocking injunction where “a substantial amount of material has been, is being or is likely to be made available in infringement of copyright”, or where a location “facilitates” such behaviour. However these sections were subsequently repealed on the basis that copyright holders already had the ability to use Section 97 of the Copyright, Designs and Patents Act to take court action against websites.
The provision of WiFi access is clearly an increasingly popular service, and the number of public libraries offering this has grown rapidly since Batt’s (2009) summary. Fewer libraries filtered their WiFi access than did their static connections, but this may just be a case of technology lag. In one instance, at least, the library service made it clear that they perceived the external providers of WiFi as carrying the responsibility for its use (or misuse). Indeed, what can be accessed via WiFi services has been strongly influenced by government policy which has led to filtering at source by most public WiFi providers. Research to date, however, suggests that blocking of pornographic content on public WiFi hotspots appears to be somewhat unreliable (Adaptive Mobile, 2013), although it should be taken into account that this research was commissioned and carried out by the providers of wireless network security software. From our desk research, BT WiFi appears to stand out in its desire not to identify itself as an aggressive censor of Internet content: whilst requiring users to adhere to the terms and conditions of their provision, it states clearly that “it is not our intent to monitor, control, or censor communications on the BT Network” (BT WiFi, n.d.).

A measure that appeared to be seriously lacking in attention was that of user education with regard to appropriate and safe Internet use, as well as training for staff in handling this aspect of Internet provision. Many of our case study respondents working on the front line of public Internet provision reported having had little or no training in this difficult area since they undertook the ECDL (or similar) on introduction of the People’s Network PCs, or since their initial induction period into their role. This is a serious omission as it appears to leave staff lacking in confidence or knowledge when supporting users. The use of volunteers to support users, whilst valuable in terms of increasing the support available and the empowerment gained by volunteers, has also possibly undermined the level of attention given to education of users with regard to appropriate use. The potential for user and staff education to facilitate the maintenance of acceptable use, supported by the implementation of an AUP, seems to have been given a much lower priority than has been given to reliance on the automated ‘blunt instrument’ solution that is represented by the implementation of filtering software. Moreover, education of personnel and users with regard to the procedures for unblocking sites also seems to be somewhat ad hoc, thus leaving some users unable to access relevant and legitimate information that has been erroneously blocked, and unable or unsure how to go about getting sites unblocked.

One overarching theme that emerged from the findings is the lack of standardisation or harmonisation across services with regard to Internet provision. This was apparent with regard to software choice and procurement; charges for services; decision-making powers; provision for minors etc. This lack of harmonisation underpins the ‘Universal Offers’ initiative being steered by a partnership of the Society of Chief Librarians, the Arts Council England and the Reading Agency. Its Universal Offer for Digital Information declares that:

“As a baseline every public library service should provide:

- Free Internet access (for a minimum period of time)
- Clear and accessible online information about library services
- Staff trained to help customers access digital information” (SCL, 2014, n.p.)

This is an excellent start in a move towards more equitable levels of service, but still does not address equality of access to content, and there is no guidance regarding filtering of content. The recommendations of the current project are intended to address this lack.

Another overarching theme that emerged from the research was the extent of dependence from sectors of the population on the Internet services provided by the public library. This was particularly apparent with regard to e-government services. A number of users reported having been sent to the
public library from the job centre to access the Universal Jobmatch site
(https://www.gov.uk/jobsearch) in order to demonstrate active job searching. From our interviews with users, it became quickly apparent that in the 21st Century, the United Kingdom still suffers from a marked digital divide, supporting statistics that report that 4 million households in Great Britain do not have Internet access (Office of National Statistics, 2013). Internet provision at the public library was seen by many of the users at our case study sites as playing a pivotal role in critical activities such as job searching, applying for jobs and claiming benefits. Given the current context of closure of public libraries, increased reliance on community libraries run by volunteers and reductions in opening hours and/or services offered, at the same time as more citizen-government transactions are taking place online, it would appear that policy in this area is disjointed and likely to be storing up trouble for the future. Whilst beyond the remit of this particular research project, we envisage that future research is needed to determine how these two divergent policy trends can better be reconciled.

To summarise the discussion therefore, this project has demonstrated conclusively that access to Internet content in UK public libraries is almost universally restricted through the implementation of filtering software. The maintenance of ‘acceptable’ use is also supported via a range of other measures such as AUPs and monitoring of use. The ubiquity of filtering software as a primary solution appears to have occurred within a vacuum of professional debate on the subject, and levels of transparency of decision-making and awareness of measures in place appear low. The findings of this project are intended to stimulate debate and raise awareness with regard to good practice that will enable public libraries to continue to offer full and open access to information, whilst also respecting the safety, autonomy and privacy of their users.
CONCLUSIONS
This section returns to the original research questions that gave rise to the MAIPLE project and outlines the conclusions of the research in the light of the questions and the findings of the research.

RQ.1. What measures are used by public libraries to regulate Internet content access, and how extensive are they?

Our findings indicate that the key strategy used by UK public libraries in this respect is the use of filtering software (100% of services responding to our questionnaire), together with the implementation of an Acceptable Use Policy (98.8% of responding services), to which users usually have to ‘click’ to commit prior to use of public Internet access. A level of regulation – and self-regulation – is also achieved through the use of auditable booking-in processes and monitoring procedures. Less attention appears to be given to user training and education, although some minimal levels are generally offered.

RQ.2. What are the problems, if any, raised by these measures for those charged with managing public Internet access?

A somewhat surprising finding was the relatively high levels of satisfaction expressed by library personnel and users alike with regard to the use of filtering software, which was generally seen as an appropriate constraint on content in the context of a public space. A majority of librarians reported finding it to be an effective solution to problems of managing acceptable use. Nevertheless, the case studies also provided examples of blocking of access to legitimate information (over-blocking), and of failure to prevent access to offensive content (under-blocking). Librarians generally appeared to regard any conflict between their professional ethic of promoting access to information and the withholding of access to content from filtering as an inevitable, necessary and acceptable compromise. AUPs were also seen as an important means of ensuring mutual understanding with regard to the purpose and scope of services provided, as well as offering a level of protection to the host services, but were not generally well promoted and in many cases it appeared that library users did not read them prior to agreeing to abide by the stated terms and conditions.

RQ.3. Is there any impact on the library user's freedom of access to information as a result of these measures?

As described above, a significant number of examples were found whereby users were prevented from gaining access to legitimate information as a consequence of the use of filtering software. Librarians also reported over-blocking as the most significant failing of the use of filtering software. In some cases, whole categories of information were blocked, such as content available on social networking sites. Perhaps more importantly, content necessary to combat social exclusion such as job hunting sites and e-government services were reported to be inaccessible. Users were not generally confident in asking for sites to be unblocked, and library personnel often lacked either the authority or the knowledge to enable them to be unblocked.

RQ.4. How effective are the measures in regulating access to inappropriate or illegal content?

Once again, filtering software, in particular, was found to be an imperfect solution, with many reports of users accessing pornographic, and in some cases illegal, content, despite such categories of material being notionally blocked. In some services, despite the use of filtering software, law enforcement agencies had to be involved in cases of misuse of facilities. In addition, the use of AUPs
appears currently to serve mainly as a means of protection for the services themselves rather than for moderating use and users, the majority of whom do not familiarise themselves with the content of such policies.

RQ.5. How could the management of public Internet access be improved to ensure stronger legal compliance without impacting adversely on freedom of enquiry?

Our overwhelming conclusion to this question is that much greater emphasis needs to be given to staff training with regard to helping users to make safe and appropriate use of Internet facilities – many of our interviewees highlighted the lack of up-to-date training to which they had had access. The same can be said with regard to training in copyright compliance: many library personnel reported not being confident in their own knowledge in this respect, or their ability to identify misuse, and, in some instances, there was evidence of an approach that could include ‘turning a blind eye’ when it was expedient so to do. In addition, much more attention needs to be paid to the education and support of users with regard to the safe and effective use of the Internet. It also became clear that the processes for getting sites that are restricted by filtering software unblocked, where appropriate, need to be made much simpler and more transparent.

RQ.6. Are minors (i.e. those under 18 in the UK) being adequately protected from online dangers such as predatory adults or exposure to adult content?

In general, it would appear that the public library remains a relatively safe and protected space for minors. Either our respondents were reluctant to report incidents of identified risk to minors or these had not been experienced. Users also did not indicate that this had been a problem. However, there are no grounds for complacency, and it is clear that the use of filtering software alone is not sufficient to guarantee protection from predatory adults or exposure to adult content: education in safe Internet use (at home, at school and in the public library), and vigilance on the part of library personnel, remain key to the safety of minors when using library Internet facilities.

RQ.7. Are the measures currently being taken the most cost-effective available, or are there more cost-effective solutions that could be adopted?

While the scope of the project did not permit full cost-benefit analyses to be carried out with regard to a range of alternative solutions, it would appear from our findings that library personnel are relatively satisfied with the effectiveness of filtering software as a solution and we did not find any reported complaints with regard to disproportionate costs. This may, however, be a result of such costs being subsumed within the IT budget of their parent institutions, or as part of the wider package of service offered by their Internet Service Provider. Resource issues were most apparent when it came to providing education and support for users: the point was made many times that library staff do not have the time to provide the levels of assistance that would be required for users to become more self-sufficient and confident in their use of library Internet facilities. However, we would conclude that more could be done with regard to the presentation and promotion of AUPs and the conditions under which Internet facilities are made available: and this could be done with relatively little cost attached.

RQ.8. How can librarians prevent the infringement of copyright that results from clients’ downloading or file-sharing activities?

Whilst we found some evidence of library personnel trying to prevent unlawful breaches of intellectual property rights, as noted above (RQ.5) many personnel did not feel confident in their
ability to prevent infringement of intellectual property rights. There is clearly a need for more training in this aspect of digital provision. Although filtering software was often used to block file-sharing sites, it was clear from our findings that infringement is still taking place and that a multi-pronged approach needs to be taken, including blocking of such sites, education of users, and greater vigilance and dedicated training of staff.

RQ.9 What specific problems have arisen for public libraries as a result of the advent of social media (e.g., social networking sites), and how are these currently being addressed?

It was clear from some of our case study findings that public libraries have been challenged by the advent of social media – and in particular, with regard to protecting minors from inappropriate content. In at least one instance, attempts to resolve this issue had been made by the wholesale blocking of social networking sites. However, as noted in our discussion this risks the alienation of a significant proportion of potential public library users, with damaging impact on the viability of the future of the service. We would again recommend the provision of appropriate user education as a more effective and satisfactory solution.

RQ.10 How can public librarians be protected from legal liability as a result of their clients’ actions?

Our findings suggest that local authorities are already very aware of the need to protect their staff from legal liability: indeed, in some instances this, together with the desire to avoid reputation damage, has perhaps led to an overly cautious response on their part with regard to the extent of content that is blocked. We would suggest that a combination of an appropriate legal disclaimer in the terms and conditions of the Acceptable Use Policy (to which users must be required to agree before gaining access to computer facilities); an enhanced focus on staff training (particularly with regard to digital copyright infringement and its prevention); and continued filtering of content offers satisfactory protection. However, we would also recommend that the latter measure should not be set at overly restrictive levels, and should be transparent in its implementation. It should also be accompanied by a clear and satisfactory unblocking mechanism for staff to use in cases of inappropriate blocking of content.

RQ.11 What lessons can local authorities learn from practice elsewhere including from the commercial provision of public Internet access?

The overwhelming message for local authorities from our findings is that insufficient attention is being paid to library staff training and preparation for the management of public Internet access. Whilst filtering appears to be standard practice and well-accepted in the UK, attitudes towards filtering and what constitutes ‘acceptable use’ are inevitably culturally constituted. Thus, the absence of filters in the majority of Scandinavian public libraries appears unproblematic to policy-makers and practitioners in those jurisdictions. With regard to comparison with commercial WiFi providers, the desk research indicated the extensive use of AUPs/ terms and conditions of use, as well as filtering of content in most outlets, thus mirroring provision in public libraries. Measures in place in this area of provision were also found to be heavily influenced by recent UK government policy with regard to default filtering of wireless Internet content (the so-called ‘family-friendly WiFi’ initiative).

In 2013, a number of high profile announcements were made in relation to public WiFi in the UK following on from developmental work by the UK Council for Child Internet Safety (UKCCIS), a group of more than 200 organisations working in partnership to help keep children safe online. The first meeting of the UKCCIS Board was held in early 2012 and included MPs and representatives from...
industry and relevant charities working in the field. In the minutes of that board meeting three main areas of broadband were mentioned that the public WiFi project would include – retail, public places including “libraries” and private/public WiFi access (p.4). By February 2013, progress had been made with the six largest public WiFi providers in what they could do to filter adult content “who together account for upwards of 96 per cent of public WiFi provision” (p.5) and by May of the same year “All providers now either filter by default or offer business customers the choice to filter” (p.5). In the summer of 2013, the Department for Culture, Media and Sport announced at a summit on tackling child sexual abuse online, that the main public WiFi providers had pledged to offer family-friendly WiFi “in public places where children are likely to be” (DCMS, 2013). This was to have been completed by the end of August 2013 according to reports: “An agreement was also reached with O2, Virgin Media, Sky, Nomad, BT and Arqiva to apply the automatic family filters to public WiFi access points by the end of August” (Strange, 2013). According to UKCCIS Board notes from July 2013, “the WiFi work only filters pornography”. It would therefore appear that public library content is now largely aligned to that of commercial ‘hotspot’ provision when it comes to filtering (albeit in some Public Library Services the content that is blocked appears to be more extensive and involving broader categories of content), and there are no clear lessons for local authorities to be derived from our analysis of this sector.

RQ.12 What additional benefits (if any) does free, public, supported Internet access in public libraries confer above commercial provision?

Our findings highlight the critical importance of public, supported Internet access in a policy arena that is focussing on the electronic delivery of government services and that is aiming for full public engagement with electronic government transactions. This is even more true given the continuing digital divide both in terms of access to infrastructure and to digital skills. The role of library personnel as mediators between people and information appears to be stronger than ever in the digital world. Without access to the Internet in public libraries it was clear that many of our case study (user) participants would be further disadvantaged: prevented from applying for jobs, benefits and government services, they would also lack the opportunity to keep up with the skills development needed to adapt to technological change. This finding is further endorsed by the recent DCMS report from an independent panel led by William Sieghart, which concluded ‘At the moment, at least 20% of the population have no digital technology at home, and far more fail to understand how to make the most of what they do have’ (Department of Culture, Media and Sport, 2014, p.6). ‘Free’ WiFi access in coffee shops, public transport and the like is not really free: it requires the purchase of a drink, or a train ticket etc. The public library is free, and our case study participants all told us how much they valued being able to visit and use the computer facilities.

Reflections on research limitations
The quantitative survey attracted a response rate of 39% of Public Library Services. Whilst this might be considered a reasonable result, and sufficient to draw some generalised conclusions for the wider population of Services (Bell, 1993), it does not enable us to give an absolute percentage for the number of Services that are using filtering software. In particular, it may be that services which do not employ filtering software (if any) would be less inclined to respond to a survey on how internet access is managed, although we have no evidence that this is the case. In hindsight, it may have been more useful to have used the Freedom of Information Act, as per the work of Brown and McMenemy in Scotland (2013), in order to establish precisely how many PLS employ filtering; however, using a questionnaire allowed us the opportunity to explore the issues in more depth. A combination of FOI request and questionnaire may have proved the optimum methodological approach for ensuring comprehensiveness of data in terms of both breadth and depth.
Similarly, although our five case studies enabled the collection of rich and illuminating data from five different Services, all of whom varied in characteristics and context, it is not possible to say that we have done more than ‘focus on one instance (or a few instances) of a particular phenomenon with a view to providing an in-depth account of events, relationships, experiences or processes occurring in that particular instance’ (Denscombe, 2003, p.32) and it would be useful to be able to extend this work further. Nevertheless, we believe that the triangulation gained from our mixed methods approach of desk research, questionnaire survey and case studies, and the validation gained for our results from practitioners and policy makers who attended the end of project workshop all lend rigour and credibility to the conclusions drawn from our findings.

Finally, we found that the interviews that we carried out with users of public library Internet facilities were far more revealing about the purpose and nature of this use than perhaps we had anticipated. We aim to follow up this work with further research in order to be able to provide recommendations for practitioners and policy makers with regard to how their services may continue to develop in order better to meet future user requirements.
RECOMMENDATIONS

Findings from the project suggest that, irrespective of the professional and ethical commitment of librarians to extend access to information without barriers or boundaries, filtered access to the Internet is now the norm in UK public libraries. Filtering of Internet content appears to be regarded by most public library practitioners as a pragmatic and necessary means of fulfilling our duty of care to library patrons (and staff). However, the findings also suggest that filtering of content is acting as a barrier to legitimate use of the Internet for library patrons, and is restricting access to ‘all publicly available information, whether factual or fiction and regardless of media or format, in which its users claim legitimate interest’ (CILIP, 2005). We also found low levels of transparency and understanding with regard to what content restrictions were in place, and how (or whether) they could be lifted for individual patrons. In many instances, staff as well as patrons, were unaware of, or lacking in confidence with regard to, content filtering and unblocking processes.

Therefore, the following recommendations are proposed in order to assist and guide Public Library Services in fulfilling their professional commitment to provide the fullest possible access to information whilst also ensuring a duty of care to their patrons. These recommendations were presented to participants at the end of project workshop and were broadly endorsed.

1. Any content filtering in place for material accessed by adults should be set at the lowest possible level for all categories of material (excepting illegal content such as child pornography, which should be blocked at source);
2. Adult content should not be restricted to the level deemed appropriate for minors. Wherever possible, a separate area should be provided for use by minors so that the risk of inadvertent viewing of content more suited to adults is minimised.
3. It is accepted that content accessed by minors should be subject to more stringent restrictions, but should still not impose undue levels of censorship. The legitimate aim of any library service should include the education of patrons such that they are able to exercise appropriate judgement in the selection of materials used/viewed. By blocking all access by minors to ‘challenging’ content, the opportunity to broaden horizons and the ability to learn to exercise discretion and evaluation in terms of what is useful and reliable information is lost. Public libraries should not be imposing levels of censorship that inhibit genuine enquiry whether on the part of adults or of minors.
4. There should be a simple, transparent and effective mechanism for having sites unblocked, that demonstrates respect towards the individual user. Library personnel should receive appropriate training and authority in the unblocking of sites, so that patrons are not prevented from accessing legitimate content.
5. There is a need for much greater transparency and openness about the use of filtering. Patrons and library personnel should always be aware of content restrictions in place, and the rationale for their imposition.
6. Much greater attention needs to be paid to education and training both of patrons and library personnel. Those responsible ‘on the ground’ for oversight of use of public library Internet use should receive appropriate (and regular) training, so that they are in a position to support and inform patrons with regard to acceptable use, and any measures in place to facilitate this. Library users, and in particular minors, would benefit from greater attention being paid to their own education with regard to the retrieval of useful and appropriate content, and in staying safe online. This is particularly the case with regard to young teenagers and the use of social media sites – blocking such sites is more likely to lead them to believe that the public library is not the place for them, and they will seek to access the content elsewhere.
7. Surveillance and monitoring of patrons’ use of the Internet should also be kept to the absolute minimum necessary to ensure legal compliance. In addition, all patrons should be made aware of any surveillance measures in place, whether these are real-time monitoring of screens or the potential for retrospective scrutiny of website histories.

8. There is a need for more professional debate on the topic in the light of our professional ethical commitments to freedom of access to information. As hypothesised at the outset of this project, filtering software appears to have become the default solution without full and open debate about the implications and consequences of this decision. In many cases library managers appear to have accepted the decision of their parent authorities to implement filtering, without full consideration of the ethical implications of this decision.

9. There is a need for a more unified and consistent approach to managing Internet access based on nationally agreed guidelines. This aligns well with the recommendations of the recent Sieghart report (Department of Culture, Media and Sport, 2014, p.9) and its call for a national digital library network.

10. Above all, it should be widely recognised that public library Internet facilities are a highly valued service, and that they should be fully promoted and extended, particularly with regard to the provision of WiFi access. This recommendation also endorses the findings of the Sieghart report (ibid) and recognises the need for public libraries to be seen as the providers of information to the general public and not as withholders of access to information.
The MAIPLE project team have disseminated the findings of the project in a number of academic and professional journal articles as well as at international conferences. Published outputs are listed below:


In addition, the Principal Investigator gave an invited presentation of the MAIPLE project findings at an e-safety roundtable forum, hosted by CILIP in London, September 2014. Other attendees included representatives from relevant youth organisations such as Youth UK. The presentation is available online and can be downloaded at http://www.cilip.org.uk/cilip/advocacy-campaigns-awards/advocacy-campaigns/information-literacy/digital-inclusion
IMPACTS

It is too early for the full impact of the project to become clear. However, the project has led to the Principal Investigator being invited by the BBC to comment with regard to the future of public libraries. This article can be viewed at http://www.bbc.co.uk/news/uk-england-26819241.

We anticipate the major impact from the project being the development and take-up of national guidelines with regard to the management of Internet access in public libraries. This work will be based on the project findings and is taking place in collaboration with Arts Council England (ACE), as a direct result of the end of project workshop.
FUTURE RESEARCH

Findings from the project have led us to identify a number of related areas that would benefit from further research, and the project team hope to be able to engage in some (or all) of these potential areas. In particular, it is proposed that subjects for investigation should include:

1. What are the major privacy implications of measures being taken to manage Internet access in public libraries, and how do public library Internet users feel about these implications?

2. Who are the different user groups who benefit most from Internet access in public libraries, and how can their needs be better met? How can Internet access in public libraries best be deployed as a means of combatting digital and social exclusion? These questions form the basis of a funding bid currently being prepared in collaboration between Hazel Hall, Professor of Social Informatics at Edinburgh Napier University, and the MAIPLE Principal Investigator. We anticipate this being ready for submission in early 2015.

3. What other censorship challenges are UK public libraries facing in the 21st Century besides restrictions on Internet use? This question also forms the basis of a further AHRC funding bid currently being prepared in collaboration between David McMenemy, Lecturer at the University of Strathclyde, and the MAIPLE Principal Investigator. We also anticipate this being ready for submission in early 2015.

4. How can we best protect younger Internet users from harm online without unduly restricting their liberty of enquiry, and their ability to benefit from the many opportunities and information sources that they may encounter online?
BIBLIOGRAPHY


Ellis, M. (2013) Jobless forced to pay for library Internet access just as more services move online *Mirror* [online] 18.06.14. Available at: http://www.mirror.co.uk/news/uk-news/jobless-forced-pay-library-Internet-1959330


Go On UK (2012). Meet the people we’re helping. Available at: http://www.go-on.co.uk/challenge/who-were-helping


The Cloud (2012). WiFi Hotspots from The Cloud. Terms and Available at: http://www.thecloud.net/free-wifi/uk-wlan-terms-and-conditions/


APPENDIX 1: Questionnaire survey

Managing Access to the Internet in Public Libraries (MAIPLE) questionnaire

Introduction

The Department of Information Science and LISU, Loughborough University, have received funding from the Arts & Humanities Research Council to conduct a two-year study investigating the Management of Access to the Internet in Public Libraries (MAIPLE).

MAIPLE will investigate how public libraries manage public access to the Internet and potential misuse issues such as accessing unacceptable and/or illegal content. This includes the use of measures such as filtering software and Acceptable Use Policies in relation to adults and minors.

MAIPLE is the first comprehensive UK-wide study investigating this issue in over a decade. A key outcome from the study will be the identification of examples of good practice and guidance on managing acceptable Internet use in public libraries for the benefit of the sector.

We would be grateful if the most relevant person in your service could complete this online questionnaire. There are 36 questions, divided into four sections, most using multiple choice buttons with a small number of questions where you will be asked to input text. Piloting of the questionnaire has indicated it should take no longer than 15 minutes to complete.

Please submit your completed form by Friday, 8 February 2013. Please press Continue to begin the survey.

If you have any questions about this survey please contact Rachel Spacey, Senior Research Associate, LISU: r.e.spacey@lboro.ac.uk

---

Section 1: Your background

1. Which local authority do you work for?
   Select an answer
   If you selected Other, please specify:

2. What is your job title?

3. Which category best fits your role?
   - Senior library management
   - Middle management
   - Library IT
   - Local authority IT department
   - Local authority legal department
   - Library administration
   - Other (please specify):

---
Section 2: Internet access in your libraries

4. What do users need in order to access the internet on a library PC? (select all that apply)

<table>
<thead>
<tr>
<th>Library members</th>
<th>Guests</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Library borrower number</td>
<td>✓</td>
</tr>
<tr>
<td>b. Username (If different to borrower number)</td>
<td>✓</td>
</tr>
<tr>
<td>c. PIN/password</td>
<td>✓</td>
</tr>
<tr>
<td>d. Proof of identity</td>
<td>✓</td>
</tr>
<tr>
<td>e. Means of payment</td>
<td>✓</td>
</tr>
<tr>
<td>f. No authentication required</td>
<td>✓</td>
</tr>
<tr>
<td>g. Other</td>
<td>✓</td>
</tr>
</tbody>
</table>

5. If you have selected 'Other' in Q4 above, please provide details here

6. Which booking system do you use for PC use?

- Manual recording
- In-house electronic system
- Proprietary software (please state which below)
- We do not have a booking system
- Other (please specify):

If you selected 'Proprietary software' above, please state which you use here

7. Does your library service charge for Internet access? (select all that apply)

- No - it is free for everyone
- The first 30 minutes are free, then we charge
- The first hour is free, then we charge
- Visitors/non-members have to pay
- Yes - everyone has to pay
- Other (please specify):
8. Does your library service offer Wi-Fi access to the public at any of its libraries?

☐ Yes
☐ No (please scroll down to the end of this section and press Continue)
☐ Don't know (please scroll down to the end of this section and press Continue)

9. What do users need in order to access Wi-Fi? Select all that apply

<table>
<thead>
<tr>
<th></th>
<th>Library members</th>
<th>Guests</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Library borrower number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Username (if different to borrower number)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. PIN/password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Proof of identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. Means of payment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. No authentication required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g. Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10. If you have selected 'Other' in Q9 above, please provide details here

11. Does the hotspot (Wi-Fi internet access) provide:

☐ Filtered access to the Internet
☐ Unfiltered access to the Internet
☐ Don't know

12. Is your Wi-Fi secure e.g. WPA or WPA2?

☐ Yes
☐ No
☐ Don't know

13. Do Wi-Fi users see a special web page to log-on/authenticate before using the Internet (known as a captive portal)?

☐ Yes
☐ No
☐ Don't know
Section 3: Managing access to the Internet

a) Filtering

14. Does your library service use Internet filtering software on some or all of its public access terminals? (select one)

- Some terminals have filtering software (please give details below)
- All terminals have filtering software
- No terminals use filtering software

If you have selected ‘Some terminals have filtering software’ above, please give details here:

15. At what level was the decision about whether to install filtering software made? (select one)

- Elected members
- Local authority senior management
- Legal department of local authority
- IT department of local authority
- Library service senior management
- Library service IT staff
- Individual library / branch
- Don’t know
- Other (please specify):

If your service does not use filtering software, please go to Question 25

16. Which filtering software do you use? (select all that apply)

- Bloxx
- Bluecoat
- Cisco
- FortiGate
- McAfee
- Net Nanny
- SmartFilter
- SurfControl
- WebSense
- In-house solution
- Don’t know
- Other (please specify):
17. Which categories of content are blocked? (select all that apply)

<table>
<thead>
<tr>
<th>Category</th>
<th>All users</th>
<th>Only for children</th>
<th>Only for teenagers</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Sexual</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Violence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Extremist</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Intolerance/Hate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. Bad language</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. Social networking e.g. Facebook, Twitter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g. Webmail</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h. File sharing/peer-to-peer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. Instant messaging</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>j. Collaborative sites e.g. wikis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k. Gambling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>l. Finance/banking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m. RSS feed aggregators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n. Online gaming</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o. File download/upload</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>p. Chat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>q. Hacking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r. Personals/dating</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s. Weapons</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>t. Illegal drugs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>u. Spyware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v. Criminal skills</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>w. Proxy avoidance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x. Blogs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>y. Television e.g. 40D, BBC i-Player</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>z. Other</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

18. If you selected ‘Other’ in Q17 above, please provide details here

19. What is the procedure for requesting a change to the library Internet filter e.g. unblocking an individual website? (select all that apply)

- [ ] Ask a member of staff in the library
- [ ] Complete a form online
- [ ] Complete a paper form in the library
- [ ] Email the library service
- [ ] Other (please specify):
20. Who has responsibility for responding to requests for changes to the library Internet filter?  
(select all that apply)

- Local authority senior management
- Legal department of local authority
- IT department of local authority
- Library service senior management
- Library service IT staff
- Library service frontline staff
- Don't know
- Other (please specify):

21. How are library users made aware of the use of filtering software?  
(select all that apply)

- Library membership form/pack
- Acceptable Use Policy
- PC/Internet use form
- Log-in screen on PC
- Information on the library website
- Posters in Library
- Other (please specify):

22. Have library users made any complaints about the filtering software in the last 12 months?  

- Yes
- No
- Don't know

If yes, what were the subjects of the complaints? (select all that apply)

- Objection to use of filtering software
- Over-blocking i.e. user unable to access legitimately required content
- Under-blocking i.e. content was accessible which user felt should be blocked
- Technical limitations of access (e.g. inability to download/upload/file share)
- Other (please specify):

23. How useful, in your opinion, is filtering software in maintaining acceptable use?  

- Very useful
- Somewhat useful
- Not very useful
- Not at all useful
- Don't know

24. Are you aware of Internet users circumventing the filters?  

- It happens a lot
- It sometimes happens
- It rarely happens
- It never happens
- Don't know
### b) Acceptable use

**25. Does your library service have a formal statement or policy regarding appropriate use of the Internet, often called an Acceptable Use Policy (AUP)?**

- [ ] Yes
- [ ] No (please scroll down to question 29)
- [ ] Don’t know (please scroll down to question 29)

  a. If yes, who was involved in its formulation? *(select all that apply)*
  - Elected members
  - Local authority senior management
  - Legal department of local authority
  - Library service IT staff
  - IT department of local authority
  - Library service senior management
  - Individual library / branch
  - Don’t know
  - Other *(please specify):*

  b. If yes, who formally approved it/signed it off? *(select one)*
  - Elected members
  - Local authority senior management
  - Legal department of local authority
  - Library service IT staff
  - IT department of local authority
  - Library service senior management
  - Individual library / branch
  - Don’t know
  - Other *(please specify):*

**26. What measures are used to draw users’ attention to the AUP? *(select all that apply)***

- [ ] Library membership form/pack
- [ ] PC/Internet use form
- [ ] Log in screen on PC
- [ ] Information on the library website
- [ ] Posters in library
- [ ] Other *(please specify):*

**27. Are you aware of any major breaches of the AUP in the last 12 months?**

- [ ] It happens a lot
- [ ] It sometimes happens
- [ ] It rarely happens
- [ ] It never happens
- [ ] Don’t know

  If yes, have these related to: *(select all that apply)*
  - Viewing of obscene (legal and illegal) content
  - Viewing of racist, extremist or hate content
  - Viewing of violent content
  - Online bullying/harassment
  - Extortion
  - Copyright infringement
  - Spamming
  - Hacking
  - Malware/viruses
  - Other breaches

  i. If ’other breaches’ selected above, please specify here
28. Are you aware of any minor breaches of the AUP in the last 12 months?

- It happens a lot
- It sometimes happens
- It rarely happens
- It never happens
- Don't know

   If yes, have these related to: (select all that apply)
   - Viewing of obscene (legal and illegal) content
   - Viewing of racist, extremist or hate content
   - Viewing of violent content
   - Online bullying/harassment
   - Extortion
   - Copyright infringement
   - Spamming
   - Hacking
   - Malware/viruses
   - Other breaches

   i. If 'other breaches' selected above, please specify here

29. What additional measures have your libraries implemented in order to maintain acceptable and/or legal use? (select all that apply)

- Internet training for library users
- PCs physically located so other library users can see them
- Visual monitoring by library staff
- Monitoring software
- Collection of Internet use data/history
- Booking system for use
- Other (please specify):

30. Do front line staff undergo regular training relating to Internet misuse?

- Yes
- No
- Don't know

**c) Protection of minors**

(defined as children and young people under 18 years of age in England, Wales and Northern Ireland and under 16 years in Scotland)

31. What measures do you take to protect minors when using the Internet in your libraries? (select all that apply)

- All terminals have filtering software
- Provision of dedicated terminals with filtering software
- Provision of dedicated area with oversight by library staff
- Provision of tailored user education
- Reliance on adherence to AUP
- Reliance on parental oversight of use
- Other (please specify):

32. Have there been any incidents involving minors and inappropriate use in the last 12 months?

- It happens a lot
- It sometimes happens
- It rarely happens
- It never happens
- Don't know
d) Best practice

33. What do you think has worked particularly well with regard to managing public access to the Internet in your service?

34. Please use this space if you would like to add any further comments about public access to the Internet in your service.

Section 4: Follow up and case study interest

35. We may wish to follow up some of your answers with an email or telephone query. If you are happy to be contacted, please give your details here:

<table>
<thead>
<tr>
<th>a. Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. Email address:</td>
</tr>
<tr>
<td>c. Telephone number:</td>
</tr>
</tbody>
</table>

Note that these details will be used only in conjunction with such additional queries, and will not be released to any third party.

36. We are planning to carry out case study research in four library services across the UK. This would involve interviews or focus groups with selected library staff and managers who are willing to participate. We would also like to talk with some users of your library service, if they agree. Each case study service will receive a report on our findings. If your authority would be interested in taking part, please provide details of the member of staff to whom we should provide further information:

<table>
<thead>
<tr>
<th>a. Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. Email address:</td>
</tr>
<tr>
<td>c. Telephone number:</td>
</tr>
</tbody>
</table>

Please note that these details will not be linked to your questionnaire responses. Contact details will only be used for administrative purposes in connection with this survey, and will not be released to any third party. No individuals or public library authorities will be identified in the reporting of the results.

Thank you for completing the survey.
APPENDIX 2: The Workshop

A one-day workshop was held at Burleigh Court, Loughborough University, on 10th July 2014 to disseminate and test the findings and recommendations of the project, and to engage with relevant stakeholders. This was an invitation-only event aimed at senior-level practitioners (generally Heads of Service), policy makers and academics working in the field. The aim of the workshop was to ensure the reliability of the recommendations and their relevance to practice.

Attendees

The workshop was attended by 20 participants, including members of the MAIPLE project team and members of the External Advisory Board. A representative from each of the participating case studies was also invited, as were representatives from relevant organisations such as Arts Council England and CILIP. A keynote speaker, Prof. Anne Goulding (author of *Public Libraries in the 21st Century*, Ashgate, 2006) was invited from Victoria University of Wellington, to provide some international comparisons and reflection to the day. The full list of attendees on the day is provided below:

- Brian Ashley, Arts Council England
- Chris Batt OBE, University College London and independent consultant, member of MAIPLE External Advisory Board
- Carol Boswarthack, Association of London Chief Librarians
- Jeanette Castle, West Lothian Council, Chair of MAIPLE External Advisory Board
- Robert Clayton, Rutland County Council
- Louise Cooke, Loughborough University, MAIPLE Principal Investigator
- Claire Creaser, Loughborough University, MAIPLE Co-Investigator
- Chris Cullen, Lincolnshire County Council
- Guy Daines, CILIP, member of MAIPLE External Advisory Board
- John Dolan OBE, member of MAIPLE External Advisory Board
- Anne Goulding, Victoria University of Wellington (New Zealand)
- Phil Jones, The Hive (Worcester), critical friend of the MAIPLE project
- Ayub Khan MBE, Warwickshire County Council
- Adrienne Muir, Loughborough University, MAIPLE Co-Investigator
- Wendy Olphert, Loughborough University
- Alan Poulter, University of Strathclyde, member of MAIPLE External Advisory Board
- Darren Smart, CILIP Public & Mobile Libraries Group
- Rachel Spacey, Loughborough University, MAIPLE Research Associate
- Valérie Spezi, Loughborough University
- Nigel Thomas, Leicestershire County Council
manage access to the internet 120 appendix 2: the workshop in public libraries

content
the programme for the day is included at the end of this appendix.

the day commenced with a keynote lecture from anne goulding, professor of library and information science at victoria university of wellington, new zealand. entitled managing the internet in public libraries: from community access to connection and co-creation, some very thought provoking and pertinent themes emerged during the course of the lecture, which took a broad perspective on the provision of internet access in public libraries. prof. goulding noted that, whilst the issue of internet access for the majority of the population in developed countries may have been resolved, there still remains a digital divide, mainly along the lines of age and social class. those without access often lack the skills or confidence in the use of technology to benefit from the information age: this then acts as a barrier to social integration and personal development in a ‘networked society’. addressing this digital divide has the potential benefit to state economies of realising cost savings through increased digital delivery of services, as well as increased tax revenues from higher employment rates. in this respect, she noted the recognition given within the welsh digital inclusion delivery plan (welsh government, 2011) to the key role that public libraries have to play. however, she also noted that uk public library internet provision has been criticised for the lack of staff support provided for users, the lack of privacy afforded to users within the public library, and the short time limits for use imposed on users (rust, 2014), and for the irony of decisions to charge for public library internet access at the same time as pushing for more government services to move online (ellis, 2013). an alternative vision was put forward as embodied in the australian government’s digital hubs programme, which embraces a more participatory digital culture with opportunities for community co-creation of content. a similar vision was proffered with the example of auckland city libraries, encouraging members of the community to contribute memories of their own to local history digital collections. these visions offer opportunities for public libraries to use new technologies to develop new relationships with their communities; to gather new knowledge about their collections; and to create platforms for innovation from within their communities.

the key findings and recommendations of the maiple project were then presented. in particular, we highlighted the ubiquity of filtering software as a key tool of choice for managing acceptable use, alongside other mechanisms such as the implementation of aup’s, monitoring of online use and user education. attendees were mostly in agreement with the finding that, rather than arguing against filtering software as an infringement on the user’s right to access to information or the librarian’s ethical commitment to the promotion of access to information, it is viewed by librarians as a necessary precautionary and protective measure, that enables librarians to preserve the library as a ‘decent’ public space. the fact that our findings suggest that most users also appear to accept the filtering of internet content in the library as necessary and appropriate in a public library context did not appear to meet with too much surprise or challenge, either. in the light of this recognition, the key recommendations for good practice that were put forward for discussion were that:

1. any content filtering in place for material accessed by adults should be set at the lowest possible level for all categories of material
2. adult content should not be restricted to the level deemed appropriate for minors
3. it is accepted that content accessed by minors may be subject to more stringent restrictions but should still not impose levels of censorship that inhibit genuine enquiry
4. there should be a simple, transparent and effective mechanism for having sites unblocked, that demonstrates respect towards the individual user
5. we need to be more transparent and open about the use of filtering
6. There is a need for more professional debate on the topic in the light of our professional ethical commitments to freedom of access to information.

Discussion
These recommendations were broadly accepted by participants, although there was some discussion around the issue of differentiating filtering levels for adults and children. The main argument driving those who disagreed with this recommendation was that one can never be sure whereabouts minors are in the library, and with access no longer limited to fixed work stations, it is hard to ensure that minors do not come into contact with offensive content displayed on adult terminals. However, other participants felt that the potential disadvantages of limiting all content to that suitable for minors irrespective of the age of user were too great to warrant such an intrusive measure. Overall, the workshop proved to be a useful forum for both validating and disseminating the project outcomes, as well as being a very enjoyable and stimulating day.
## APPENDIX 3: Filtering of WiFi hot spots

<table>
<thead>
<tr>
<th>Company</th>
<th>Filtered</th>
<th>Provider</th>
<th>AUP/T&amp;C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Costa Coffee</td>
<td>Yes</td>
<td>O2</td>
<td>Not on the Costa website. O2 Wifi website has Terms and Conditions <a href="https://www.o2wifi.co.uk/signup/terms">https://www.o2wifi.co.uk/signup/terms</a></td>
</tr>
<tr>
<td>McDonalds</td>
<td>Yes</td>
<td>O2</td>
<td>McDonalds website – Restaurants – Free Wifi – FAQs - Terms and Conditions are “found on the landing page when you connect to the WiFi service in a McDonald's restaurant”. First company to join the Mumsnet Family Friendly WiFi programme which filters <a href="http://www.mcdonalds.co.uk/ukhome/Restaurants/FreeWiFi.html">http://www.mcdonalds.co.uk/ukhome/Restaurants/FreeWiFi.html</a> O2 Wifi website has Terms and Conditions <a href="https://www.o2wifi.co.uk/signup/terms">https://www.o2wifi.co.uk/signup/terms</a></td>
</tr>
<tr>
<td>Debenhams</td>
<td>Yes</td>
<td>O2</td>
<td>Debenhams website – Store Services – Free Wifi. No Terms and Conditions or mention of filters. O2 Wifi website has Terms and Conditions <a href="https://www.o2wifi.co.uk/signup/terms">https://www.o2wifi.co.uk/signup/terms</a></td>
</tr>
<tr>
<td>Pizza Hut</td>
<td>Yes</td>
<td>O2</td>
<td>Not on the Pizza Hut website. There is a brief section in the FAQs which notes that most of the restaurants have Wifi. <a href="http://www.pizzahut.co.uk/restaurants/about/faqs/">http://www.pizzahut.co.uk/restaurants/about/faqs/</a> O2 Wifi website has Terms and Conditions <a href="https://www.o2wifi.co.uk/signup/terms">https://www.o2wifi.co.uk/signup/terms</a></td>
</tr>
<tr>
<td>House of Fraser</td>
<td>Yes</td>
<td>O2</td>
<td>Not on the House of Fraser website. No mention of Wifi. O2 Wifi website has Terms and Conditions <a href="https://www.o2wifi.co.uk/signup/terms">https://www.o2wifi.co.uk/signup/terms</a></td>
</tr>
<tr>
<td>Subway</td>
<td>Yes</td>
<td>O2</td>
<td>Not on the Subway website. No mention of Wifi. O2 Wifi website has Terms and Conditions <a href="https://www.o2wifi.co.uk/signup/terms">https://www.o2wifi.co.uk/signup/terms</a></td>
</tr>
<tr>
<td>Argos</td>
<td>Yes</td>
<td>O2</td>
<td>Not on the Argos website. No mention of Wifi. O2 Wifi website has Terms and Conditions <a href="https://www.o2wifi.co.uk/signup/terms">https://www.o2wifi.co.uk/signup/terms</a></td>
</tr>
<tr>
<td>Greggs</td>
<td>Yes</td>
<td>The Cloud, BSkyB/Sky WiFi</td>
<td>Not on the Greggs website. No mention of Wifi. The Cloud has Terms and Conditions for Wifi in the UK on its website: <a href="http://www.thecloud.net/free-wifi/uk-wlan-terms-and-conditions/">http://www.thecloud.net/free-wifi/uk-wlan-terms-and-conditions/</a> and notes that some sites may be blocked.</td>
</tr>
<tr>
<td>Pizza Express</td>
<td>Yes</td>
<td>The Cloud, BSkyB/Sky WiFi</td>
<td>Pizza Express website – Customer Services – FAQs – search for WiFi – states they have WiFi provided by The Cloud. No Terms and Conditions or mention of filters.</td>
</tr>
<tr>
<td>Library</td>
<td>Access Options</td>
<td>WiFi Providers</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>M&amp;S</td>
<td>Yes</td>
<td>The Cloud, BSkyB/Sky WiFi</td>
<td>Not on the M&amp;S website. No mention of WiFi. The Cloud has Terms and Conditions for Wifi in the UK on its website: <a href="http://www.thecloud.net/free-wifi/uk-wlan-terms-and-conditions/">http://www.thecloud.net/free-wifi/uk-wlan-terms-and-conditions/</a> and notes that some sites may be blocked.</td>
</tr>
<tr>
<td>WH Smith</td>
<td>Yes</td>
<td>The Cloud, BSkyB/Sky WiFi</td>
<td>Not on the WH Smith website. No mention of Wifi. The Cloud has Terms and Conditions for Wifi in the UK on its website: <a href="http://www.thecloud.net/free-wifi/uk-wlan-terms-and-conditions/">http://www.thecloud.net/free-wifi/uk-wlan-terms-and-conditions/</a> and notes that some sites may be blocked.</td>
</tr>
<tr>
<td>Wetherspoon</td>
<td>Yes</td>
<td>The Cloud, BSkyB/Sky WiFi</td>
<td>Wetherspoon website – pubs – contact us – customer services – FAQs – WiFi. No mention of Terms and Conditions of filtering. Refers to The Cloud: <a href="http://www.idwetherspoon.co.uk/home/faqs">http://www.idwetherspoon.co.uk/home/faqs</a> The Cloud has Terms and Conditions for Wifi in the UK on its website: <a href="http://www.thecloud.net/free-wifi/uk-wlan-terms-and-conditions/">http://www.thecloud.net/free-wifi/uk-wlan-terms-and-conditions/</a> and notes that some sites may be blocked.</td>
</tr>
<tr>
<td>Network Rail</td>
<td>Yes</td>
<td>BT WiFi AND The Cloud, BSkyB/Sky WiFi AND T-Mobile</td>
<td>Pay as you go WiFi is available at a number of Network Rail operated stations provided by BT and The Cloud. Some stations also offer WiFi from T-Mobile. Information about WiFi is detailed under facilities at individual stations. There is no mention of Terms and Conditions or filtering but links are provided to BT, The Cloud and T-Mobile websites.</td>
</tr>
<tr>
<td>John Lewis</td>
<td>Option to</td>
<td>BT Openzone/ BT WiFi</td>
<td>John Lewis website – Inspiration and Advice – Access WiFi in our shops: <a href="http://www.johnlewis.com/inspiration-and-advice/access-Wifi-i-in-our-shops">http://www.johnlewis.com/inspiration-and-advice/access-Wifi-i-in-our-shops</a> No mention of Terms and Conditions or filtering. Refers to BT Openzone. BT WiFi has an AUP in its Terms and Conditions section: <a href="http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp">http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp</a></td>
</tr>
<tr>
<td>Starbucks</td>
<td>Option to</td>
<td>BT Openzone/ BT WiFi</td>
<td>Starbucks website – Coffeehouse – Wifi United Kingdom: <a href="http://www.starbucks.co.uk/coffeehouse/wireless-Internet">http://www.starbucks.co.uk/coffeehouse/wireless-Internet</a> No mention of Terms and Conditions or filtering. Refers to BT WiFi. BT WiFi has an AUP in its Terms and Conditions section: <a href="http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp">http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp</a></td>
</tr>
<tr>
<td>Company</td>
<td>Access Type</td>
<td>WiFi Provider</td>
<td>Access Information</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Burger King</td>
<td>Option to</td>
<td>BT Openzone/</td>
<td>Not on the Burger King website. No mention of WiFi. BT WiFi has an AUP in its Terms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BT WiFi</td>
<td>and Conditions section: <a href="http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp">http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp</a></td>
</tr>
<tr>
<td>Hilton Worldwide</td>
<td>Option to</td>
<td>BT Openzone/</td>
<td>Details of WiFi availability are shown within the information for individual hotels. No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BT WiFi</td>
<td>mention on the main website of WiFi, Terms and Conditions or filtering. BT WiFi has</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>an AUP in its Terms and Conditions section: <a href="http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp">http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp</a></td>
</tr>
<tr>
<td>Fenwick</td>
<td>Option to</td>
<td>BT Openzone/</td>
<td>Details of WiFi availability are shown within the information for individual stores with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BT WiFi</td>
<td>the BT WiFi logo. No mention of Terms and Conditions or filtering. BT WiFi has an AUP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>in its Terms and Conditions section: <a href="http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp">http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp</a></td>
</tr>
<tr>
<td>GAME</td>
<td>Option to</td>
<td>BT Openzone/</td>
<td>Not on the GAME website. No mention of WiFi. BT WiFi has an AUP in its Terms and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BT WiFi</td>
<td>Conditions section: <a href="http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp">http://www.btwifi.com/terms-and-conditions/acceptable-use-policy.jsp</a></td>
</tr>
<tr>
<td>Boots</td>
<td>Option to</td>
<td>Unknown</td>
<td>Boots website – Help – About Boots.com – Questions – Boots WiFi includes Terms and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Conditions - Boots reserves the right to block access and content of certain sites at</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Boots would not disclose who provides their WiFi.</td>
</tr>
<tr>
<td>Travelodge</td>
<td>Comply with</td>
<td>Arqiva</td>
<td>Travelodge website – Contact us – General enquiries/questions – Facilities – Do you offer wireless Internet access: <a href="http://support.travelodge.co.uk/link/portal/15071/15090/Article/1167/Do-you-offer-wireless-Internet-access-WiFi-in-rooms">http://support.travelodge.co.uk/link/portal/15071/15090/Article/1167/Do-you-offer-wireless-Internet-access-WiFi-in-rooms</a> No mention of Terms and Conditions or filtering. Individual hotel details include WiFi information. No mention of Terms and Conditions or filtering. Refers customers to Arqiva if there are problems.</td>
</tr>
<tr>
<td>Brewers Fayre</td>
<td>Comply with</td>
<td>Arqiva</td>
<td>Not on the Brewers Fayre website.</td>
</tr>
<tr>
<td></td>
<td>client’s</td>
<td></td>
<td>requirements. If none specified, family friendly filtering default.</td>
</tr>
<tr>
<td>Heathrow Airport</td>
<td>Yes</td>
<td>Arqiva</td>
<td>Heathrow airport – heathrow airport guide – Airport directory – WiFi – WiFi at Heathrow FAQs: Is Heathrow’s WiFi “family friendly”? Yes. The WiFi service that Arqiva provides to Heathrow uses third-party filtering software. This means that it will automatically block access to certain types of websites and content which it deems to be inappropriate.</td>
</tr>
<tr>
<td>Company</td>
<td>Filtering Default</td>
<td>WiFi Provider</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>---------------</td>
<td>-------</td>
</tr>
<tr>
<td>Asda</td>
<td>Yes</td>
<td>EE</td>
<td>Not on the Asda website. Not on the EE website.</td>
</tr>
<tr>
<td>London Underground</td>
<td>Yes</td>
<td>Virgin Media</td>
<td><a href="http://my.virginmedia.com/wifi/index.html">http://my.virginmedia.com/wifi/index.html</a> - FAQs - The Service - Does Virgin Media block any content on WiFi on the London Underground? It does not say that it does explicitly, rather “As WiFi on the London Underground is a public WiFi network, Virgin Media has a responsibility to ensure that the content available is suitable for young people to access themselves or to look at over someone else’s shoulder”.</td>
</tr>
<tr>
<td>Virgin Trains</td>
<td>Unclear</td>
<td>Nomad Digital</td>
<td>Not on the Nomad Digital website. Virgin Trains Wifi FAQs do not refer to filtering. They do urge users “please do not view content that others may find offensive or inappropriate”. Access to some sites is restricted on the grounds that they may breach copyright.</td>
</tr>
</tbody>
</table>
End of Award Report Submitted to the Arts & Humanities Research Council
Grant: AH/J005878/1