IFLA 2014 LYON

Submitted on: 16/07/2014

Towards a public library standard for acceptable use of computing facilities

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

Abstract:

Acceptable use policies (AUPs) in public library services are important documents. They act both as guides to acceptable use of facilities for library users, and protection for the library service against any abuse or misuse of these facilities. Through their role as quasi-legal documents, they also have the potential to both promote access to the library service, and hinder it. How can we be sure all users understand the implications of an AUP? How can language within them be made easily understood while still offering protection?

Such documents are relatively new governance concerns in public libraries, the need for them brought about with the advance of computing and internet facilities in public libraries throughout the 1990s and 2000s. As such there is little in the way of literature or research on their implementation, and only a handful of authors discussing best practice in their design.

This paper adds to the general dearth of material on this important topic. Utilising a discourse analysis methodology, the paper compares differences in AUPs in terms of length, content, and tone. Presenting a range of examples from the United Kingdom, this paper highlights the key issues that the profession should be concerned about regarding design of AUPs, and focusses on how language and tone can be a potential barrier to engagement for users. Can a workable document be developed that is sharable across geographic regions?

The paper finishes with suggestions as to how we can collectively progress workable AUPs that help the library users understand their responsibilities when using computing facilities, while allowing the library service to feel secure in provision of the service.

Keywords: public libraries, acceptable use, computing facilities, internet, standards

Introduction

The Acceptable Use Policy (AUP) is one of the most important interface documents between the user and the library in the modern era. While managing the parameters of access to the services provided, it also acts as a guide to users as to what is expected of them when using the facilities.

This paper reports results from a pilot study analysing 20 AUPs for UK library services aimed at discovering several aspects of their design and implementation. Firstly it will gauge differences in length of the documents, and secondly it will analyze the language utilized in them for consistency of structure, and also tone. Does the tone of the AUPs offer negative or positive connotations to users from the point of view of their use the service? Alternatively, does the AUP act as a barrier to accessing a service due to its tone?

This pilot study will inform the methodology of a project funded by the Scottish Library and Information Council to develop a Scottish-wide AUP that could be used by all public libraries in the region. The PAUL Project (Policy development for Acceptable Use in Libraries) runs from July 2014 to March 2015.

Research and policy context

AUPs can and often do differ in length, style and tone. While guidance exists on how best to design an AUP, ultimately the design and implentation of an AUP document is something that is done locally. Therefore the organisation implementing it must be sure that it represents a proper agreement between it and the library user, one that has a proper legal basis and that can be relied on to ensure protection for the organisation if the rules are breached. Equally, as librarians, we have an ethical duty to ensure our users are properly informed regarding the services they are provided with.

When signing a legal document, users should be made aware of the nature of it and what is expected of them as users, and what they can expect from our organisations. In a study conducted in 2007 by the author, 12 different public library services across the UK were visited by a researcher seeking to access the Interent as a non-member. In only 1 of the services visited was the AUP explained to the researcher, and perhaps more worryingly, in 2 of the services the library staff bypassed the AUP for the researcher by clicking the log-on banner (which acted as the agreement to adhere to the AUP) on their behalf (McMenemy, 2008, p.487). It is doubtful in either of the 2 cases whether the researcher could have been held liable for any misuse of the service.

Advice on AUP development

This section of the paper will highlight some of the advice that has been offered in the literature regarding good practice in AUP design. As far back as 1994 Scott and Voss designed their 7 Ps model for the design of computing use policies. Clearly this was an era before mass access to the Internet, however some of the issues from 1994 remain relevant. The 7 Ps were:

1. Participation: who is involved in the design of the policy
2. Partitioning: the design of the document vis a vis distinct sections.
3. Philosophy: what the facility can be used for (in Internet terms, what can be accessed)

4. Privacy: what level of privacy can be expected?
5. Persnickety: what are the do's and don'ts when using the service
6. Phog Phactor: ensuring readability of the document
7. Publication: how is it going to be communicated to users?

We can still see the relevance of all of these themes today, since they focus on designing a broad-based policy that clearly sets out parameters of use, while remaining accessible to the user who signs it.

Laughton has undertaken a hierarchical analysis of AUPs and suggests that:

> It is impossible for an effective AUP to deal with every clause and remain readable. For this reason, some sections of an AUP carry more weight than others, denoting importance (Laughton, 2008).

He suggests that an AUP has 3 main purposes:

> 1. Educating users about activities that may be harmful to the organization
> 2. Providing legal notice of unacceptable behaviour and the penalties for such behaviour
> 3. Protecting an organization from liabilities it may incur from misuse of the Internet and other computer facilities (Laughton, 2008).

Highlighting the key point that an AUP must respect user rights as well as protecting the organisation, he goes on to suggest that "A well-rounded policy is carefully planned and includes input from and consideration by all parties involved including staff, members, legal representatives and external experts" (Laughton, 2008). He highlights that AUPs that are "confusing and written as if they were specifically targeted at lawyers and legal professionals" are less effective than those that are designed with the user in mind.

Kelehear has also offered advice as to contents of an effective AUP, which it is suggested should include:

1. Statement on the intended use and an outline on the advantages of the Internet
2. List of responsibilities for users
3. Code of conduct administering the use of the Internet
4. Description of what constitutes acceptable and unacceptable use of the Internet
5. Disclaimer absolving the organization from possible responsibility of any misuse of the Internet (Kelehear, 2005, p.33).

Sturges presented a schema for an effective AUP in his 2002 study of public internet access in libraries. Containing 7 key elements, he suggests a range of areas that should be covered for effectiveness:

1. Aims and objectives – not perhaps as straightforward as it may initially seems. What is the purpose of the service? Is it purely educational, or is recreational use allowed?
2. Eligibility – Who the service is provided for? How do young people access, and with whose permission?
3. Scope – The limits of the service.

4. Illegal use – An understanding of the types of use that against the law in the geographic region.
5. Unacceptable use – A description of what is deemed unacceptable by the particular institution.
6. Service commitments – The services that will be provided by the particular institution.
7. User commitments - Any agreements that must be adhered to by the user. (Sturges, 2002, p.122-123)

Sturges highlights that it has become more common for organisations to refer to their AUP documents in more generic terms such as 'Internet Use Policy' or 'Codes of Conduct'; acknowledging that while AUP is a familiar term, it is also a potentially loaded one.

Methodology

For the purposes of this paper and to highlight the issues involved, we have selected Sturges' (2002) schema to code our sample of 20 UK public library AUPs. This has been selected because it is a synthesis of a range of guidance documents, and thus provides a comprehensive structure. Since it was also authored in the United Kingdom (UK) by an academic researching and teaching in that environment it was therefore deemed a good fit for the purpose of this research which focuses on a pilot study of UK services.

20 AUP documents were selected randomly from those publically available on the websites of UK public library services. A simple Google search was conducted for acceptable use policies in UK public libraries. To ensure geographic coverage related to the ration of country size, 3 were selected from Scotland, 2 from Wales with the remaining coming from English regions. All libraries have been anonymized for this study, since it is not the intention of the author to highlight individual libraries for criticism, but instead raise broader issues that are of concern to the sector as a whole.

All 20 AUPs were imported into NVivo software for qualitative analysis, and coded using the schema above. Another important element of the exercise was to ascertain how the AUPs communicate their message to users. To this end, discourse analysis was applied to each document, analysing how the themes were presented from the point of view of behaviour deemed to be acceptable and unacceptable. As one of the key researchers in discourse analysis has observed, "language is an irreducible part of social life, dialectically interconnect with other aspects of social life, so that social analysis and research always has to take account of language (Fairclough, 2003, p.2). In addition, as has also been observed, discourse analysis is an under-used method in library and information science, thus the usage of it in this study is relatively novel (Budd, 2006).

Results

Of the 20 AUPs analysed the number of pages of each document varied in the range from one page long to nine pages long (Figure 1).

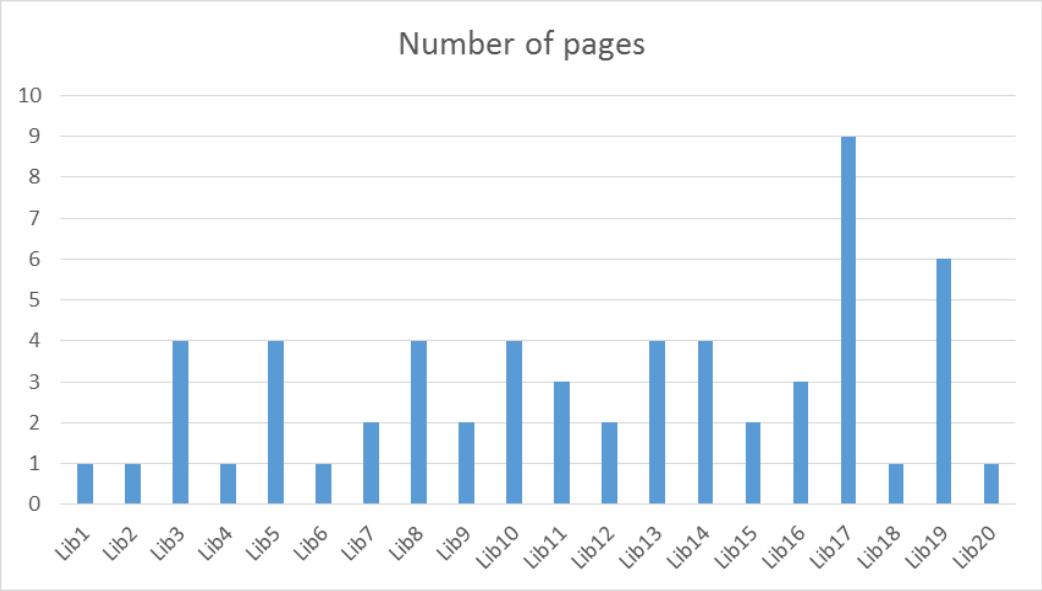

Figure 1

The length of a document will understandably be an issue for some users who have to read and understand the document before they sign it. Making the document as short as possible while ensuring it covers the key areas should be an important goal.

Aims and objectives

In terms of aims and objectives of providing the service, there was a general consistency as to why the service was offered across authorities:

- Lib 8: "to support the educational, information and cultural needs of the community."
- Lib 10: "the educational, recreational, information, cultural and communication needs of the community."
- Lib 12: "to support educational and community information resources. Priority may be given to customers wishing to access such material."
- Lib 13: "provide free access to the Internet as part of its role to enable access to information, recreation, culture and lifelong learning opportunities for its customers."
- Lib 15: "provides free public access to the Internet and other computer resources as part of its role in providing access to information, education and leisure opportunities for the whole community and as part of its commitment to supporting lifelong learning."

This consistency of mission is important, since it confirms that the services country-wide are all basing their provision under similar themes. This would then lead us to question later, if evidence presents itself, any restrictions on access that clash with these aims.

Eligibility

Eligibility for use of the service was generally consistent across the libraries, however it was clear that some restricted access to registered users, while others allowed non-members to also utilise the service. While this kind of decision is clearly a local one, it does seem unusual that some authorities support citizens from outside of the geographic area in accessing the service, while others do not. An inconsistency was also found between those who charged for access to the ICT facilities and those who did not. Clearly, charging for access to the Internet is a potential barrier to use for those on fixed or low incomes.

Scope

The scope of the service as defined in AUPs primarily emphasised the Internet access available. However some of the authorities highlighted other important services that were provided via the ICTs, as follows:

- Lib 1: "provide public access to the Internet, MS Office and a range of ICT facilities."
- Lib 5: "provides public computers in libraries for use by customers and permits the use of personal portable digital devices in some libraries. Wi-Fi is also available in some libraries."
- Lib 9: "We provide access to the World Wide Web, a range of audio, video and other plug- ins, and standard Microsoft Office software. You can use web-based email and we will show you how to set up and manage an email account."

An important point was raised in the analysis by focussing on scope. Libraries rarely looked beyond Internet access in their definition of the scope of the service, which missed out a lot of excellent and potentially useful services the ICTs provided for users. This emphasis is arguably understandable, since the key risk to the library service comes from the Internet; however from a user perspective defining a broader scope as to why the facilities are provided could offer users a deeper understanding of the potential of the service in their lives.

Illegal use

When it came to illegal use, the AUPs often cited specific legislation that was of concern to the library services:

- Lib 1: Users should "Not attempt to bypass security systems to gain unauthorised access to any computer. Any attempt to do so is an offence under the Computer Misuse Act 1990 (c. 18) and the individual may be liable to prosecution"
- Lib 7: "you are bound to the relevant UK law, including the Data Protection Act 1998; Parts of the Criminal Justice and Public Order Act 1994; Computer Misuse Act 1990; Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002, and agree to abide by it. It is your responsibility to familiarise yourself with all Statutory requirements."
- Lib 10: "you are reminded that it is your responsibility to comply with this legislation including: Copyright, Designs and Patents Act 1988 • European Copyright Directive 2001 • Computer Misuse Act 1990 • Data Protection Act 1998"

- Lib 11: “This Acceptable Use Policy is informed by City Council Policy and the following legislation: The Obscene Publications Act 1959 and 1964 • The Copyright, Design and Patents Act 1988 • The Data Protection Acts • Computer Misuse Act 1990”
- Lib 17: “This includes not using the IT facilities in any way which may result in a breach of the Copyright, Designs and Patents Act 1988 and the European Copyright Directive 2001 and Copyright and Related Rights Regulations 2003; Data Protection Act 1998; The Civic Government (Scotland) Act 1982; Sexual Offences Act 2003 (as applicable); Public Order Act 1986; Computer Misuse Act 1990; Human Rights Act 1998 (all as amended); and any other local, regional, national and international law, order or regulation.”

While making users aware of their responsibilities and the law they may be liable to breach is clearly important, it would seem that merely rhyming off specific Acts of Parliament serves a limited role. For the layperson such legislation is likely to be dense, and it would be appropriate for the library service to synthesise such material in a more accessible way. Not doing so risks the user signing a document that they have not understood.

Unacceptable use

The focus on unacceptable use in the documents tended to focus on specific types of material that users should guard against accessing. For instance material that is:

- Lib 1: “obscene, homophobic, racist or unlawful - is pornographic or could cause offence to others - is in breach of copyright”
- Lib 15: “Creating, sending or storing any abusive, offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material Harassment in any form (including sexual and racial harassment) Infringement of copyright under the provisions of the Copyright Act 1988”
- Lib 17: “users must not use indecent, obscene, offensive, or threatening language in any form of electronic communication including e-mail messages, electronic forms, and blog postings”
- Lib 18: “The facilities may not be used for any of the following: 1. to access obscene or indecent material, or material that is likely to cause significant offence to others; 2. The creation or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material; 3. The creation or transmission of material which is designed to or likely to cause annoyance, inconvenience or unnecessary anxiety”

Again there was a consistency here in terms of use deemed as unacceptable, focussing on terms such as offensive or obscene. The term offensive, however, is arguably subjective, and an AUP would be more efficient if it attempted to define what is deemed to be offensive for that community. Interestingly, Lib 8 attempts to counter this somewhat by informing users in their AUP that it “is not opposed to satire or controversial thought as such, but only sites whose content would, if circulated, interfere with the freedom of others to a greater extent than acceptable in a democratic society, are defamatory, pornographic etc.” The reference to satire being acceptable is a minor, but important, attempt at highlighting freedom of thought.

Service commitments

Service commitments tended to be limited in the policies examined; since the focus was primarily on the acceptable use of Internet access, the wider scope of why the ICTs were provided were largely ignored. It would seem that an AUP should clearly describe exactly what the ICTs provided can be utilized for, and not doing so risks the danger of under-use.

User commitments

The emphasis here was on attempting to ask the user to take responsibility over their use of the service. Lib 4 revealed that it "provides a level of filtering for adult users, but you must also take responsibility for your own activities." Lib 10 also emphasised the responsibility of the user as a member of the community:

> We would like you to be aware of the needs of others who are also using the computers, respect their privacy, to behave in a manner that doesn't disrupt their use and enjoyment and to be responsible in your use of the equipment and facilities in our libraries. We try to prevent customers accidentally accessing sites containing or promoting illegal or offensive content. Please do not deliberately search for, or distribute, illegal or offensive content.

There were also other examples of calls for the user respecting the community in their use of the service:

- Lib 8: "Reporting illegal sites - If you see something you suspect is illegal online report it at www.iwf.org.uk"
- Lib 16: "Library users must respect the privacy of other users, and refrain from attempting to view or read material being used by others"

We can see the library services attempting to respect the user as individuals and request they take responsibility as individuals in using a community service. This is potentially a positive way of passing on responsibility to users that does not patronise them.

Parameters of acceptable and unacceptable behaviour

It is also useful for us to examine the tone of how acceptable and unacceptable behaviour is communicated to the users in the AUPs. We have already highlighted the point that terms such as offensive and obscene were common in terms of what is deemed unacceptable, however there was very little in the AUPs that specified what *acceptable* use was.

Lib 6 determined acceptable use "as (but not limited to): Research • Email • Online retail • School work, and • Homework." This is a limited range of activities in the everyday information seeking of citizens. Lib 8 offered that "We encourage you to access legitimate information on the Internet" and continued it "does not prohibit specific online activities as long as they are not considered to be illegal, offensive, obscene, abusive or troublesome to other computer users."

Unacceptable behaviour was far more prevalent in terms of definition within the AUPs, and the tone this was presented in various ways. While admittedly a difficult concept to communicate, there were occasions when the vagueness of the definition was potentially confusing. Some examples are highlighted below:

Lib 2: “The creation, display or transmission of material which is designed or likely to cause annoyance, inconvenience, unnecessary anxiety, threats or the promotion of violence.
Lib 4: “I will not use the computer for sending material likely to cause offence or inconvenience”
Lib 7: Accessing “material which is offensive in any way whatsoever”

A term like *inconvenience* is extremely vague. For instance, an elected official receiving an email complaint from a constituent could deem the complaint inconvenient, even when legitimate. Would such a scenario run the risk of the user being banned from using the facilities? Additionally, suggesting it is a breach of an AUP to access “material which is offensive in any way whatsoever” runs the risk of a myriad of legitimate information sources being deemed inappropriate. Websites on evolution may be offensive to a creationist – would this be potentially challengeable? Common sense would say no, however if an AUP is written in such a fashion, it potentially poses a risk that the library service may receive such challenges. A tighter focus on the AUP design could negate this risk.

One of the most challenging aspects of managing Internet access is around the issues of monitoring and filtering of access (Brown and McMenemy, 2012; Poulter et al, 2009). In the AUPs examined there was a consistent approach to ensuring the user was aware that content was filtered, and their use was monitored. How this was done, however, reveals an important aspect of tone. Some AUPs balanced the rights of the user with the filtering policy:

- Lib 1: we “reserve the right to monitor these services, and where deemed appropriate keep logged records of ICT use in accordance with the Data Protection Act 1998.”
- Lib 4: “We may monitor your use of the computer, including websites visited, in order to plan better services and to ensure you keep to this policy. We will not use personal information for any other purpose, or divulge it to other people or organisations, in accordance with the Data Protection Act 1998.”

This is a sensible tactic, since it reinforces that while monitoring may be necessary, it is done so with cognisance of the rights of the citizen. Other AUPs painted monitoring and filtering in more negative tones:

- Lib 2: “If staff are in doubt about a user's intentions they will be entitled to ask that user to cease using the Council's computer facilities.”
- Lib 9: We filter access “to reduce the risk of your finding sites which are not appropriate in a public library. These include an ‘intolerance’ filter which restricts access to sites which promote the more extreme views which adherents feel are part of their faith or belief.
- Lib 16: “monitor computer logs showing access to Internet sites, and any public access of illegal, offensive or controversial material may be the subject of further action. Monitoring of computer usage can be performed electronically and manually.”

When issues of monitoring and privacy of use are at stake, it is important for the library service to communicate this to users in such a way that it is not off-putting. Presenting this negatively potentially reflects on the image of the service. As a service that historically relies on a conception of privacy between the citizen and the library, communicating to them that their use of the service is now open to unspecified monitoring necessitates a sensitive approach.

Advice for users

Linked to the above, and an important aspect of tone, is how the AUP offers advice to the user. The AUP is able to get across important pointers as to how the user can be careful in their use of the service, for instance:

- Lib 1: "Be aware that the library is a public place and that in the interest of personal security customers are strongly advised not to broadcast personal or private details over the Internet. Confidentiality cannot be assured whilst using the libraries' ICT facilities."
- Lib 10: "Be safe on the web - If you have epilepsy, or suffer from any condition that may be affected by using a computer, use is at your own risk. If you find yourself feeling unwell while you're working on the computer please end your session and, if necessary, ask a member of staff for assistance….. Please be aware that subscribing to websites and entering or broadcasting personal or private details over the internet may lead to you receiving unwanted mail or attention. Always be sure to read the terms and conditions attached to any website you subscribe to. Families, children and young people should also be aware of other internet safety issues."
- Lib 12: "For your own security and privacy, we advise you not to use library computers to broadcast personal details, including online financial transactions."

In these examples we see an important duty of care evident from the library services. While the AUP must ensure the protection of the library service, it can also be used to communicate sensible precautions to users who may be new to using ICTs. In these cases we see positive use of the documents to interact with and educate users.

Discussion

Our pilot study has revealed consistent issues with regards how AUPs for public libraries are designed and utulised. While the emphasis on protecting the library service from liability is an important one, what is of equal importance is ensuring policies are designed that are consistent, understandable, and promote the service in the most positive way possible.

What seems clear from the evidence so far is that while we have a clear idea related to the appropriate structure of AUP documents, we understand less how to make the documents accessible to a broad range of users. In a public library context this is of vital importance, since the library serves the largest range of users of any other type of library. We cannot assume a universal understanding of the contents of an AUP document, and merely listing specific laws we do not expect our users to breach is not enough to ensure they understand exactly what those laws mean. There is arguably an unfair transfer of legal and ethical responsibility to users on crucially important factors that the library service could do much more to ensure an understanding of.

We can design policies that ensure users take responsibility for their online behaviour, and the importance of this cannot be understated. Equally, however, we can use the policies to educate and inform users as to the best use of ICT facilities, ensuring they can confidently access the services.

The author would suggest further research into the development of generic AUPs is vital; not merely from the point of view of templates or suggestions of wish lists for what they should

contain, but towards a more forthright adoption of a standard for what a universal service could look like. What exactly does computer and Internet access in a public library mean for all citizens in a geographic region?

Conclusions

Access to computing facilities and the Internet are vital factors in the role of the public library as a social equalizer. We must get over the understandable fear that providing this service brings, and move forward confidently understanding what we expect of the service, our users, and what they can expect of us. There is no reason that all public libraries in a single geographic region, subject to the same laws and same mores, should not have the same AUP. By a collective pooling of effort and an agreement on service standards we could create a document that is widely understood and could act as an advocacy tool for the services we provide. At the moment we have a situation where every public library service usually develops their own document, which as well as offering a duplication of effort, also muddies the waters with regards to what we as a profession tell the world we do. There is no ethical reason why a postcode lottery should exist in terms of the access citizens receive to ICT services in public libraries, and the development of a single standard for AUPs would go a long way to creating a truly universal understanding of this exciting, but challenging, area of service.

Acknowledgments
The author gratefully acknowledges the support of the Scottish Library and Information Council who have funded the PAUL project to investigate the development of a national AUP for Scottish public libraries that runs from July 2014 to March 2015.

References

Brown, G.T. and McMenemy, D. (2013) 'The Implementation of Internet Filtering in Scottish Public Libraries.' *Aslib Proceedings.* 65(2) pp.182-202

Budd, J.M. (2006) 'Discourse Analysis and the Study of Communication in LIS.' *Library Trends.* 55(1) pp.65-82

Fairclough, N. (2003) *Analysing Discourse: Textual analysis for social research*. London: Routledge.

Kelehear, Z. (2005) "When Email goes bad: be sure that your AUP cover staff as well as students." *American School Board Journal* January: pp.32-34.

Laughton, P.A. (2008) 'Hierarchical Analysis of Acceptable Use Policies.' *South African Journal of Information Management.* 10(4) Online Journal Available from: http://www.sajim.co.za/index.php/SAJIM/issue/view/34 Accessed on 5/6/2014

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

Poulter, A., Ferguson, I., McMenemy, D. and Glassey, R. (2009) 'Question: Where Would You Go to Escape Detection if You Wanted to Do Something Illegal on the Internet? Hint:

Shush!' *Global Security, Safety and Sustainability Communications in Computer and Information Science.* 45 pp.1-8.

Scott, V. and Voss, R. (1994) "Ethics and the 7 'P's of computing use policies." *Ethics in Computing Age*: 61-67.

Sturges, P. (2002) *Public Internet Access in Information and Library Services.* London: Facet