

# SECURITY ENHANCEMENT IN PUBLIC ICT SERVICES IN WALES

Nick Robinson<sup>1</sup> and Stuart Cunningham<sup>2</sup>

<sup>1</sup>Wrexham County Borough Council, Wrexham, North Wales, UK  
[nick.robinson@wrexham.gov.uk](mailto:nick.robinson@wrexham.gov.uk)

<sup>2</sup>Centre for Applied Internet Research (CAIR), University of Wales, NEWI, Plas Coch Campus, Wrexham, North Wales, UK  
[s.cunningham@newi.ac.uk](mailto:s.cunningham@newi.ac.uk)

## **ABSTRACT**

*This paper investigates and establishes current and planned best practice for implementing ICT security within public libraries Wales. These investigations lead to the identification of security policies and practices across and range of public ICT services. We show that there is a range of practices currently employed across various local authorities within Wales. Given that each of these local authorities is part of a larger, national network infrastructure, we recommend that a large-scale security policy be considered to ensure uniformity and compliance across all of the local authorities. The findings of our investigation act as foundations for forming a cohesive policy and indicate areas of current common practice which may lead forward future developments.*

*The investigation highlights opportunities for Welsh local authorities to enhance the ICT security service, particularly in the areas of: plans for dealing with security issues, standardisation of security products and policies, adequate security training for ICT support staff and measures for reporting security incidents.*

## **KEYWORDS**

*ICT, Security, Policies*

## **1. INTRODUCTION**

In 2002 each local authority in Wales had the opportunity to receive grant money from the Welsh Assembly to provide computer network links to all their public libraries. The computer network links were to feed back to a location where the local authority had a connection to the Internet. The grant money also included for the provision of computers, software, other peripheral devices, furniture, and crucially, the cost of security measures.

At around the same time grant money became available to provide a network for public libraries, money was also made available to provide similar services to secondary and primary schools throughout Wales[1]. The schools network would be in two parts. Part one concentrated on providing a network between schools within the boundaries of each local authority. Part two concentrated on linking all local authorities together, onto what is known today as the Lifelong Learning Network Wales (LLNW). The LLNW would then connect to SuperJanet, the higher and further education network and eventually global Internet. Figure 1 shows a diagram of the Welsh LLNW backbone [2].

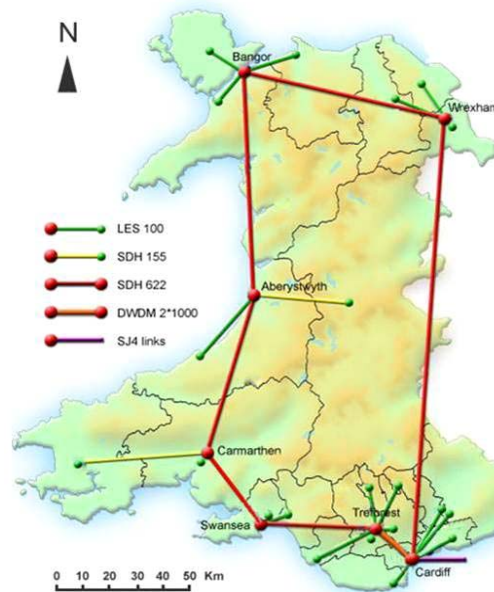


Figure 1. Welsh Local Authority Lifelong Learning Network Wales (LLNW)

For Internet services, all school connections were to find their way back to the core of the local authority's network, then go out to the Internet via the LLNW connection: an identical requirement to the public libraries. A big advantage of connecting all sites back to the network core is that enterprise-wide systems can be implemented at the core and delivered to any connected site, making it financially feasible to put in place effective and efficient computer security systems.

Once the computer network was in place, local authorities began providing members of the public with free Internet access, provided they were members of one of the libraries and agreed to the library Information and Communication Technology (ICT) Acceptable Use Policy (AUP).

Over three years have passed since the framework was implemented. During that time thousands of people have used ICT facilities within public libraries. As the IT industry continually identifies security holes, newly identified vulnerabilities, exploitable security weaknesses and threats from the Internet, it is beneficial for local authority ICT staff to continue to enforce strong security policies and protection [3].

Each local authority is responsible for conducting their security implementation at public libraries. Local authority ICT departments are able to involve organisations who deliver consultation and implementation of computer services whilst considering the security of the ICT system. These two factors have led to various configurations in delivering ICT services for libraries across Wales.

There are no global guidelines issued to local authorities as to what security measures should be introduced as part of their ICT services with public libraries. Without guidelines or best practice, some local authorities may be providing ICT services within public libraries which are less secure than other local authorities. This shows clear disparity, which is unusual in an otherwise centrally controlled infrastructure. This paper investigates to what extent there is inequality in security practices between local authorities and as a result of this research identifies and proposes policies and standards to be considered for adoption across Welsh local authorities.

## **2. CURRENT ICT SECURITY PRACTICES**

### **2.1. Overview of Security Requirements**

ICT security can be broken into three areas: Computer Security which focuses on protecting information stored computer, Network Security which focuses on securing of the use of the organisations network and data communications facilities and Internet Security which focuses on the security requirements needed for business data processing using geographically dispersed interconnected networks [4].

ICT security is prevention, detection and reaction to unauthorised actions by users of computer systems. ICT security is about protecting valuable computer-related assets including ICT hardware, software, storage media, data and people that an organisation uses to perform computing tasks [5]. Security in public ICT services in particular intrinsically implies a broad spectrum of security issues; attacks can potentially take form from the most cutting-edge software and network attacks to the theft and abuse of hardware, components and equipment.

In addition the risks of identity theft are also of concern, especially when a diverse and large quantity of users may use a common system. This produces heightened awareness of information management issues and increased need for adhesion and compliance with current Government legislation, including The Data Protection Act (1998) and The Human Rights Act (1998) as well as other indirectly related legislation.

### **2.2. General Security Procedures**

ICT departments restrict the use of ICT resources by identifying what services are available and who needs access to those services. This principle can be applied to protecting users from accessing inappropriate websites, receiving junk emails, ensuring loopholes in application software are patched and any other area where ICT security needs consideration.

Restrictions to the use of ICT are defined within an Acceptable Use Policy [7]. On the human front, the policy must define what behaviour is and is not allowed, by whom and in what circumstances. On the practical and operational front, the policy should provide the context for a supporting set of guidelines and procedures which will establish, at a detailed level, how security is implemented for all the information systems concerned. Overall the policy must define the place that information security plays in supporting the mission and goals of the organisation.

An organisation's adoption of a corporate ICT Acceptable Use Policy will contain many elements, one of these being an Internet security management programme which features an Internet security policy – itself comprising of a number of sub policies, including; an Internet information protection policy, an Internet information access policy, an Internet employee privacy policy and an Internet acceptable usage policy.

In broad terms, there are five defensive strategies which an ICT department can adopt to restrict usage of ICT [8]:

- Isolate – keep everybody out. Impractical for all but a few applications.
- Exclude – keep the bad guys out.
- Restrict – let the bad guys in, but keep them from doing damage.
- Recover – undo the damage.
- Punish – catch the bad guys and prosecute.

## 2.3. Current ICT Practices in Libraries

Information detailing ICT security designed for use in public libraries is not readily available. There are numerous books and journals which discuss ICT service provision within libraries, what should be available and what basic security protection should be implemented – but there is generally nothing technically solid by which an ICT practitioner could follow to ensure that the ICT security within public libraries is either sufficient or effectively adequate. To this end, we investigate the current state of ICT security practices within local authorities which provide public library ICT facilities within Wales.

To examine the current practices, a qualitative investigation was undertaken involving 50% of the Welsh local authorities. The broad contexts outlined for analysis roughly fell into the areas of desktop/local security, enterprise-wide security, physical security, network infrastructure security, identifying and reducing threats, and staff training.

### 2.3.1. Overview

Table 1 presents background information for each of the local authorities, gained as part of the investigation (Some figures were not disclosed by local authorities, this is denoted by “N/D”).

Table 1. Local Authority Library Demographics

<b>Local Authority</b>	<b># Libraries</b>	<b># Users</b>	<b># Computers</b>
Cardiff Council	19	132789	219
Carmarthenshire Council	35	N/D	300
Conwy Council	13	N/D	120
Denbighshire Council	8	N/D	114
Glamorgan Council	9	N/D	N/D
Gwynedd Council	17	N/D	N/D
Monmouthshire Council	6	14646	80
Pembrokeshire Council	14	38545	52
Rhondda-Cynon-Taf Council	29	112662	139
Swansea Council	18	19622	121
Wrexham Council	12	N/D	150
<b>Average (non-zero)</b>	<b>16</b>	<b>63653</b>	<b>144</b>

### 2.3.2. Desktop/Local Security

To assess to what extent the local desktop machines were secure, we look first at the primary user security ‘first-line’ measures which are in place. This incorporates investigation into the types of devices and removable media which users are permitted to use as well as the security measures employed in securing user access and protection from viruses and other threats.

The allowance of removable media is often a primary cause of the infection and spread of viruses and other software-borne problems, as well as a simple mechanism which can allow data to be copied and removed from a system. The services permitted by each authority are shown in Table 2.

Table 2. Removable Media

Local Authority	USB	CD/DVD Read	CD Write	DVD Write	FDD	Tape Drive	Zip Drive	Ext. HDD
Cardiff Council	✓	✓	✓	✗	✓	✗	✗	✓
Carmarthenshire Council	✓	✗	✗	✗	✓	✗	✗	✗
Conwy Council	✓	✓	✓	✗	✓	✗	✗	✓
Denbighshire Council	✓	✓	✓	✗	✓	✗	✗	✓
Glamorgan Council	✓	✓	✓	✓	✓	✗	✗	✓
Gwynedd Council	✓	✓	✓	✗	✓	✗	✗	✓
Monmouthshire Council	✗	✓	✓	✓	✓	✗	✗	✓
Pembrokeshire Council	✗	✓	✗	✗	✗	✗	✗	✗
Rhondda-Cynon-Taf Council	✓	✓	✓	✗	✓	✓	✗	✗
Swansea Council	✓	✓	✓	✗	✓	✗	✗	✓
Wrexham Council	✓	✓	✓	N/D	✓	✗	N/D	✓

As Table 2 shows, CDs and DVDs are the most used/permitted type of portable medium, with USB devices closely following behind. Tape and Zip drives are the least used/permitted. This may be due to the technology being dated and limited in functionality/storage capacity. DVD read/write devices are also restricted in their use, which may also be an indication of their comparatively higher cost.

Table 3 shows security measures used on public access computers. It is worth noting that enterprise-wide solutions may be preferred, these are presented in section 2.3.2.

Table 3. Desktop Security Measures

Local Authority	Firewall	Anti-Virus	Anti-Virus Updates	Anti-Spyware	Browser Security
Cardiff Council	Windows	Norton	Immediate	None	None
Carmarthenshire Council	Windows	e-Trust	Twice Daily	None	None
Conwy Council	None	Sophos	Daily	None	None
Denbighshire Council	None	Trend	As needed	Trend	None
Glamorgan Council	None	McAfee	Immediate	McAfee	None
Gwynedd Council	Windows	e-Trust	Immediate	None	None
Monmouthshire Council	None	Trend	Daily	None	None
Pembrokeshire Council	McAfee	McAfee	Weekly	None	RM Safety Net
Rhondda-Cynon-Taf Council	None	McAfee	Monthly	None	None
Swansea Council	None	e-Trust	Daily	None	None
Wrexham Council	None	e-Trust	Daily	None	None

The data in Table 3 shows clear disparity between the software and security features employed by the surveyed council library facilities. In particular, the spectrum of policies applied in critical areas, such as the frequency of anti-virus update, use of firewalls, and lack in uptake of anti-spyware software indicate that there may be a need for a common policy and procedure in these areas.

Figure 2 shows an overview of additional desktop security measures in place at Welsh Local Authority libraries. The graph indicates whether or not access to the named services or configurations is actively prevented.

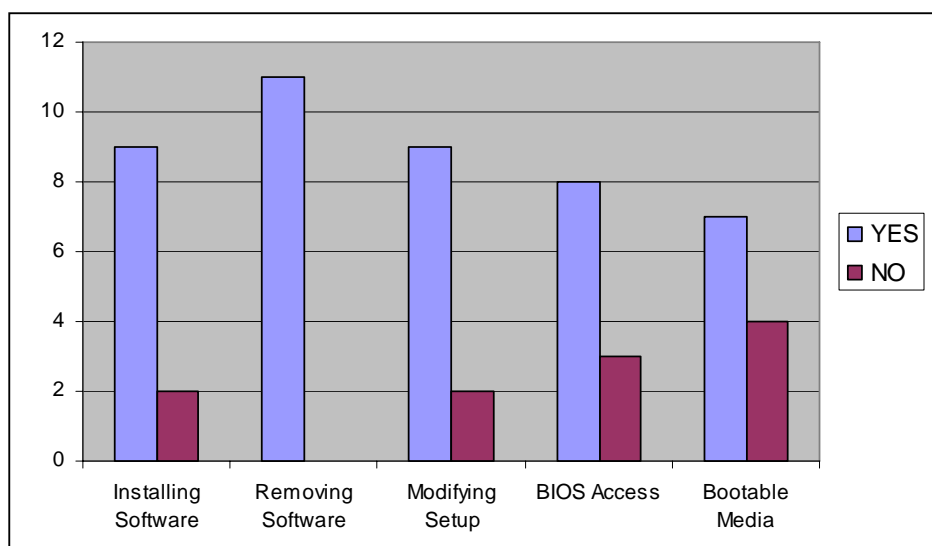


Figure 2. Prevention of Access to Services/Configuration

### 2.3.2. Enterprise-Wide Security

Given the nature and size of the network infrastructure which exists within each of the local authorities, there are also large-scale network security measures in place and deployed across the localised area. In this sub-section, we look briefly at these enterprise-wide security measures put in place across each of the local authorities to provide a bigger picture of the security measures which impact upon users across all of the sub-networks within the local authority.

Table 4 shows the enterprise-wide security measures introduced to safeguard ICT services at public libraries.

Table 4. Enterprise-wide Security Adoption

Local Authority	Firewall	Anti-Virus	Anti-Virus Update	Anti-Spyware	Browser Security	IDS System
Cardiff Council (Ca)	Checkpoint	Symantec	Immediate	Symantec	Smartfilter	None
Carmarthenshire Council (Cm)	Cyber guard	Antigen	Twice Daily	None	Web Marshall	None
Conwy Council (Cn)	Nokia	Trend	Daily	None	Websense	None
Denbighshire Council (Dn)	Nokia	Trend	Immediate	None	Websense	None
Glamorgan	Cisco Pix	McAfee	Immediate	McAfee	None	None

Council (Gm)						
Gwynedd Council (Gw)	Symantec	eTrust	Immediate	None	Surf Control	Symantec + Cisco
Monmouthshire Council (Mm)	MS ISA	Trend	Daily	None	MS ISA	None
Pembrokeshire Council (Pb)	Checkpoint	McAfee	Weekly	None	RM Safety Net	None
Rhondda-Cynon-Taf Council (Rc)	Checkpoint	McAfee	Immediate	McAfee	Surf Control	Cisco
Swansea Council (Sw)	Checkpoint	eTrust	Daily	None	Websense	None
Wrexham Council (Wx)	Checkpoint	eTrust	Daily	None	Websense	Checkpoint

Figure 3 shows an overview, across all of the local authorities, of the network security measures in place to prevent and identify internal and external threats to the network infrastructure.

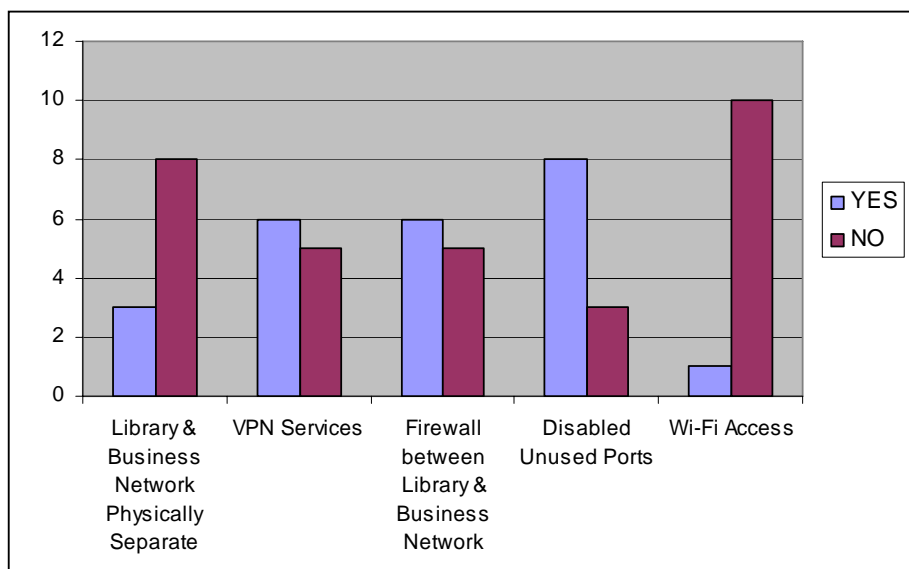


Figure 3. Network Infrastructure Security

Figure 4 shows an overview, across all of the local authorities, of the use of policies and procedures within local authority libraries to prevent, report, and obtain information regarding the misuse of security breaches in systems.

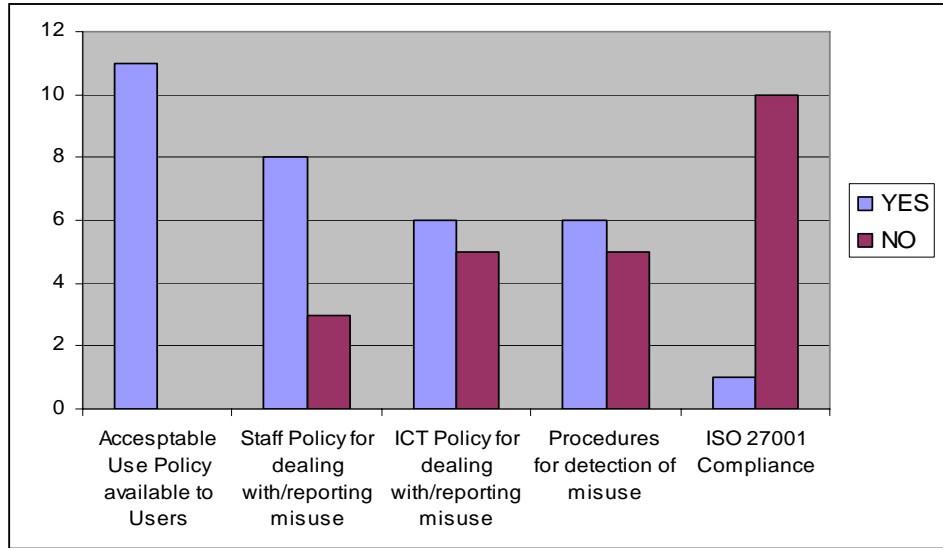


Figure 4. Reporting/Evidencing ICT Misuse

Finally, Figure 5 details the training undertaken by staff in each of the local authorities analysed. This includes staff from libraries within the local authority as well as staff from the local authority ICT department. By investigating this area we measure the depth and breadth of training which is provided to staff that have responsibility for computer security. Figure 5 details whether or not staff have received training in the named subject areas.

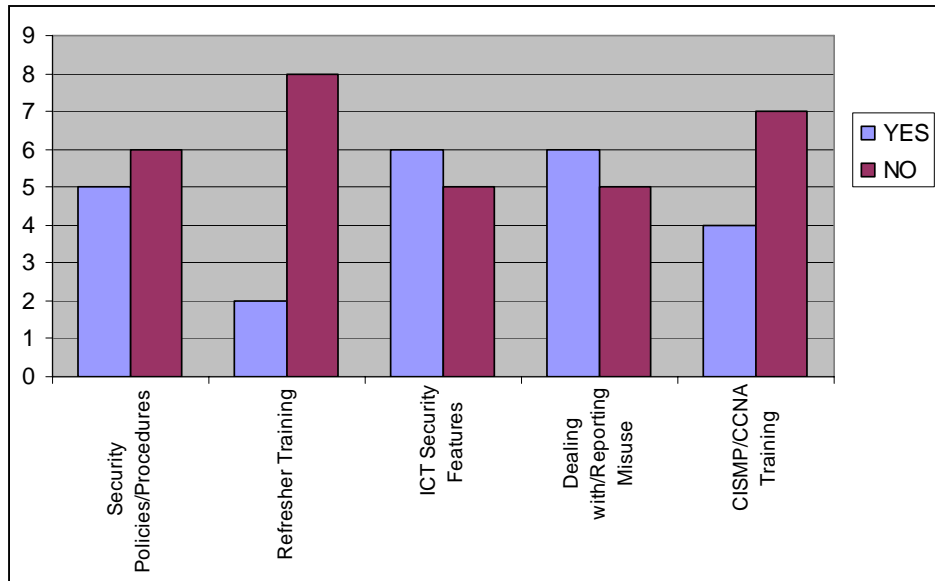


Figure 5. Local Authority Staff Training

The information gained in this section establishes that although there is disparity in practice and procedures across local authorities, there are also common approaches and tools used in the majority of cases. This leads us forwards in attempting to establish the basis and framework when attempting to define a recommended best practice to be considered by local authorities within Wales.

### **3. RECOMMENDED BEST PRACTICE**

There are currently 289 RFC documents on security, but very few with any direct relevance to ICT security within libraries. One RFC, 1244, titled Site Security Handbook written in 1991, provides a good framework for recommending best practice for ICT security in general, parts of which can be adopted for ICT security within libraries. The RFC, though covers a broad area of ICT security, does not cover all security aspects which require consideration.

The following attempts to highlight the areas of ICT security best practice specifically within libraries, but could be used for other environments whereby ICT is used. Identified areas of best practice are a combination of information obtained from the results of this study, established security literature, and current RFC documents. Identified areas of best practice are obtained from a combination of information retrieved during research into best practice, which was conducted over numerous months from up-to-date security books, journals and websites, feedback from Welsh local authorities via the use of questionnaires, which were composed using the information derived from research, information obtained from existing RFC documents and considerations identified during security testing of libraries at a Welsh local authority. Consideration is also given in developing these recommendations, to the iterative approach to security policy and procedures given by Fites, et al. [7]. The points presented provide a top-level overview of these guidelines.

#### **3.1. Local/Desktop ICT Security Measures**

Desktop security measures which should be used for public library ICT computers include:

- Access to services via uniquely identifiable password protected login account linked to the library member via membership number.
- A desktop firewall and anti-virus.
- Automatic updating of operating system and applications, and patches.
- Prevention of the installation of unlicensed software.
- Prevention of the removal or disabling of desktop and security software.
- Prevention of access to the operating system controls, including command prompt.
- Restrictions in the use of some removal media.
- Encrypted and protected data file 'save' areas.
- Enforce policies through Microsoft group and mandatory policies, lock-down software and BIOS passwords.

Any of the above desktop measures may be replaced by an enterprise-wide solution which can deliver the same level of protection from a centrally managed solution. Implementation of measures at both the desktop and the enterprise would give a tiered level of security providing extra security, especially during times of failure of one of the systems. However, in some isolated cases it may not always be practical to implement enterprise-wide measures, especially if we consider the use of these guidelines beyond the cited example of Welsh local authorities.

#### **3.2. Enterprise-wide ICT Security Measures**

- Enterprise Firewall. Common practice within Welsh local authorities.
- Enterprise URL filtering system. Common practice within Welsh local authorities.
- Enterprise anti-spyware and anti-virus systems.
- Server and desktop patch / updates management system.
- Regular security backups of key systems.
- Desktop policy management systems including remote control.
- Default system user accounts, passwords and SNMP community strings should be changed, disabled or removed.

- Monitoring, logging and management tools.
- Implement resilient enterprise-wide systems which use standby components or systems to ensure continual service such as clustered server farms and storage area networks.
- ICT security alerting services to provide early warnings of threats.
- Specialist IT security and policy/procedure training & updates for ICT support staff.

The best practice guidelines proposed should be used as a target by which ICT staff should aim towards. However, it is accepted that there will be instances when best practice targets can not be reached, either due to technological or monetary restrictions, the business risk is less than the effort, the restrictions imposed by adoption of a security measure or the practice is not applicable to circumstances.

#### **4. CONCLUSIONS**

There is a vast quantity of information available on topics of ICT security from a broad perspective. The challenge faced when implementing ICT security within public libraries is the ability to identify what security measures would be needed to successfully protect the libraries network and its users. As there has been no best practice guidelines identified specifically for public library ICT services, investigations were directed towards organisations which provided ICT security solutions, best practice and policies which addressed issues for organisations.

The research conducted within this work could be used towards adopting a strategy specifically for the Welsh local authorities detailed and even wider, towards an RFC for ICT security best practice within any library or similar public access ICT service across the UK.

Best practice, though valid in giving ICT staff a solid base to start and a checklist with pointers to security considerations during installation of a public library ICT suite, can not be produced in a definitive format due to the varying business requirements and topologies of the network and services to be delivered. What best practice guidelines can do is illustrate what is deemed to be the best way to deliver a security ICT service. The research conducted provided the necessary information to establish the best practice guidelines.

#### **ACKNOWLEDGEMENTS**

The authors would like to thank Ralph Hardy and Dave Hylands.

#### **REFERENCES**

- [1] Big Lottery Funding Research Issue 7, The People's Network: evaluation summary. Available at: [http://www.mla.gov.uk/resources/assets/P/pn\\_evaluation\\_summary\\_pdf\\_4283.pdf](http://www.mla.gov.uk/resources/assets/P/pn_evaluation_summary_pdf_4283.pdf) [Accessed April 2007]
- [2] Symberlist, R. (2002) *Lifelong Learning Network (LLN) Network Diagrams*, Welsh Networking Ltd. Available at: <http://llnmicro.wnl.net/networkdiagrams/> [Accessed February 2007]
- [3] Lemos, Robert (2006) *Security flaws on the rise, questions remain*, SecurityFocus. Available at: <http://www.securityfocus.com/news/11367> [Accessed January 2007]
- [4] Stallings, W. (2003) *Network Security Essentials*, 2nd Edition, Prentice Hall.
- [5] Pfleeger, C.P. & Pfleeger, S.L., (2003) *Security in Computing*, 3rd Edition, Prentice Hall.
- [6] Lampson, B.W., (2004) "Computer security in the real world", *Computer*, IEEE Computer Society, Vol. 37, No.6, pp37-46.
- [7] Infosec Acceptable Use Policy Guide Available at: [http://www.sans.org/resources/policies/Acceptable\\_Use\\_Policy.pdf](http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf) [Accessed April 2007]
- [8] Fites, M., Kratz, P. & Brebner, A., (1989), *Control and Security of Computer Information Systems*, Computer Science Press.