Technical Specification

Institutional Infrastructure

Version Control

Version	Description	Date
A	Document out of draft	4th November 2005
B	Current benchmark version: • Chapter 4 - Network Technologies in institutions added • Minor text changes to Executive Summary, Introduction, Scope and How to use this document sections • Chapter titles reworded • Clarification wording added for Section 2.2: Standards For Office Productivity Applications • Clarifications to SSL/s-http requirements • Appendix E updated to contain Chapter 4 design criteria	21 November 2005

Executive Summary

A well designed and maintained infrastructure is key to an institution's ability to deliver a highly effective ICT resource to the learner, educator and administrator. In order for the ICT infrastructure to be sustainable, flexible and adaptive there needs to be a common approach taken in network design, ICT resources and security. A clear standards-based approach will help to ensure that infrastructures designed today are able to offer an ICT resource to the institution that is useful today and in future years.

In this document Becta has addressed the technical specifications that are needed in order to implement the requirements outlined in Becta's 'Functional Specification – Institutional Infrastructure' (available from http://www.becta.org.uk/schools/techstandards)

Key technical design criteria for four areas of an institution's ICT are specified here; local area networks in institutions; services and applications in institutions; implementation of ICT security in institutions; and network technologies in institutions. Each area has requirements defined that are seen as necessary or highly desirable if institutions are to move their ICT resources forwards in a sustainable, coherent and reliable manner.

The current version of this specification is the result of a consultation process with a wide range of stakeholders and as such the requirements outlined here ought to be seen as achievable by institutions within the next 3-5 years.

Introduction

In its Functional Specification for Institutional Infrastructure, Becta specifies a comprehensive set of requirements from institution infrastructure that need to be accessible to in order to offer learners, educators and administrators a wide range of choice and access to ICT, support flexible working via ICT, manage data and improve efficiency and secure data and protect the user. This paper describes the technical criteria required in order to fulfil the necessary functionality outlined in Becta's Functional Specification. In order to provide a useful document relevant to all stakeholders this specification is divided into the following related, logical sections:

- Section 1 – Local area networks in institutions
- Section 2 – Services and applications in institutions
- Section 3 – Implementation of ICT security in institutions
- Section 4 – Network Technologies in institutions

Where possible, the technical specifications described here are based on open technical standards and specifications incorporating the work performed by many organisations, including BSI[1], IEEE[2], IETF[3], IMS[4], W3C[5] and Wi-Fi Alliance[6]. Implementing requirements to known and specified standards is the best way, and in many cases the only way, to ensure that the institution's infrastructure can evolve and expand in a sustainable and coherent way. A standards-based approach will also help to ensure that there can be seamless interoperability between different institutions. This will be of paramount importance as educational ICT moves into the future towards ever more integrated learning environments.

Many of the technical specifications and standards referenced here are based on those from the e-Government Interoperability Framework (e-GIF)[7]. Where there are no open standards or specifications available Becta have either attempted to facilitate agreement between stakeholders to a proposed specification or, on occasional circumstances, proposed a de facto standard as the way forwards.

Scope

This paper provides technical specifications and design criteria based on the functional requirements identified in Becta's Functional Specification for Institutional Infrastructure, which specifies a number of requirements for institution's networks and the services and applications that need to be accessible over those networks.

So as to concentrate on how the network, applications and services, the associated ICT security and network technologies can support and enhance learning, teaching and data management, specific technologies are not explicitly mentioned, neither are curriculum specific areas dealt with in detail. Funding and procurement advice are also not addressed in this document. Information on these areas is currently available from http://www.teachernet.gov.uk/management/schoolfunding/ and http://www.becta.org.uk/leaders/display.cfm?section=3.

It must be noted that this document refers to all learners and educators. Where accessibility issues are not explicitly mentioned, it is for the individual institution to decide what additional requirements may be needed for their institution.

[1] http://www.bsi-global.com
[2] http://standards.ieee.org
[3] http://www.ietf.org
[4] http://www.imsglobal.org
[5] http://www.w3.org
[6] http://www.wi-fi.org
[7] http://www.govtalk.gov.uk/schemasstandards/egif.asp

Becta's Institutional Infrastructure specifications

Becta's infrastructure specifications, frameworks and tools offer a coherent and comprehensive approach to institutional infrastructure requirements. This document must therefore be seen as part of a series of documents that support the institutional infrastructure component of Becta's National Digital Infrastructure (http://www.becta.org.uk/schools/infrastructure). The relationship of Becta's infrastructure specifications, frameworks and tools to an institution's ICT design and implementation is demonstrated in figure 1.

Functional Specification: Institutional Infrastructure

- Sets out the functional requirements for institutions to aim to achieve within the next 3-5 years. Available from http://www.becta.org.uk/schools/techstandards

Technical Specification : Institutional Infrastructure

- Supports the Functional Specification by setting out the technical specifications and requirements for an institution's infrastructure in four key areas; Local Area Networks in institutions, services and applications in institutions, implementation of ICT security institutions and network technologies in institutions

Institutional LAN matrix tool

- This is a tool that an institution can use for self evaluation processes against the requirements set out in the Functional specification. This is available from http://matrix.becta.org.uk (from December 05)

Functional Specification Procurement Guidance

- Supports the functional specification by giving institutions supplementary advice on questions to ask before implementation of a requirement takes place (available from December 2005)

Framework for ICT Technical Support

- Framework for ICT Technical Support (FITS) is a best-practice Framework for ICT Technical Support (FITS) and is available to support the delivery of ICT in education. Available from http://www.becta.org.uk/technicalsupport .

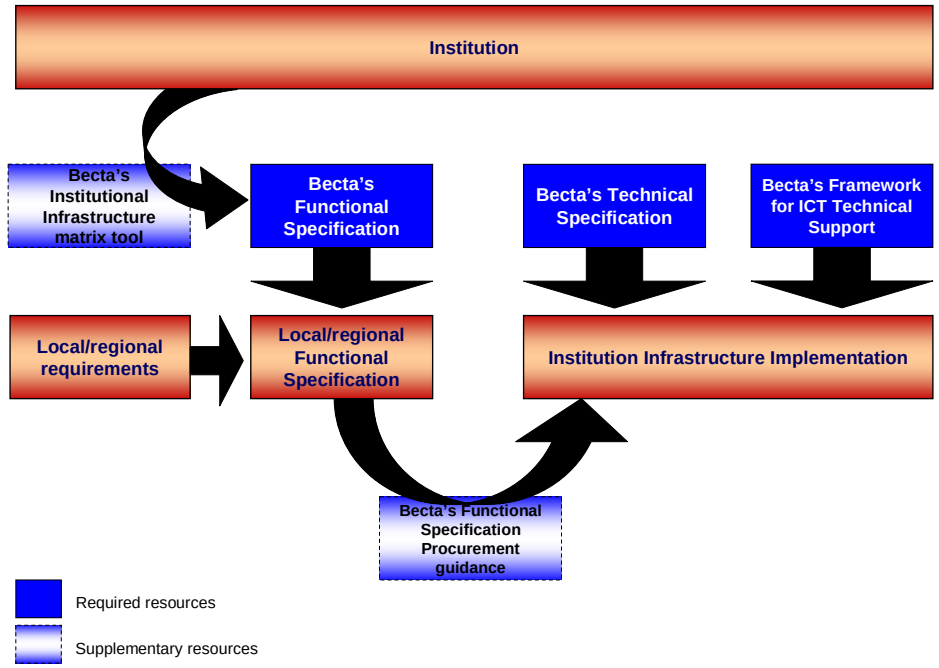

Figure 1 The relationship of Becta's institutional infrastructure documents to an institution's ICT design and implementation

Intended audience

This technical specification is written for those who have an interest and responsibilities for Institutional infrastructure at an operational and management level. It is of particular interest to ICT coordinators, network administration staff, managed service suppliers and ICT educational suppliers.

How to use this document

For an institution that is being newly built or completely refurbished, the design criteria described here provides a minimum technical specification upon which additional requirements could be added, depending on the particular requirements or specialism an institution has. For a Local Authority (LA), this could provide the basis for all the institutions to achieve the same level of ICT provision throughout the LA. For other institutions this specification could provide a checklist of the ICT provision that they already have in place and a vision of where they need to move next.

Each section begins with a general description, followed by a bullet list of "Design criteria". These design criteria are a series of requirements that address the implementation of a particular ICT provision. Where a minimum and advanced set of requirements can be easily defined, these criteria are followed by an upgrade path describing additional functionality or technical specifications that can enhance the specification. As with the other documents described above, the reader is asked to observe the Wording conventions
(below) and the Glossary of terms (Appendix D) for guidance on terminology.

Open discussion and feedback on what is set out here is encouraged from all who have an interest in educational ICT. Appendix A provides a means by which feedback can be given.

The use of standards and specifications

Implementing requirements to known and specified standards is the best, and in many cases, the only way to ensure that an institution's ICT infrastructure can evolve and expand in a sustainable and coherent manner helping to make certain that there is seamless interoperability between ICT resources. This will be paramount as institutions move forwards towards ever more integrated learning environments.

Basic principles

Within this specification there are basic principles that need to be continually considered and addressed. The following principles are of paramount importance and need to be considered (and in some cases considered as prerequisites) whenever ICT infrastructure enhancements are being planned.

- **Reliability**
  The institution's ICT infrastructure must be reliable. An unreliable infrastructure is unlikely to enhance the learning experience or aid the educator. It will become a frustration to learners, educators and administrators alike if devices, applications and services cannot be relied upon. Whilst using an infrastructure that meets Becta's technical specification will greatly aid reliability, the institution will still be responsible for checking with suppliers and providers that infrastructure components are of proven reliability.
- **Coherence**
  With the variety of technologies on offer in the marketplace, it is important that an institution ensures coherence by implementing ICT technologies that work together and fit with the overall ICT strategy. This coherence must also be applied equally to devices and services running over the institution's infrastructure and to any connection that enables effective use of the National Education Network (http://www.becta.org.uk/nen) or the Internet.
- **Affordability and Sustainability**
  Whilst institutions can often identify the immediate costs of a new ICT resource the total cost of ownership (TCO) must be considered in order for the institution to be able to sustain a

resource. Becta has carried out a considerable amount of work in this field and readers are encouraged to familiarise themselves with this (http://www.becta.org.uk/leaders/display.cfm?section=14_9_4).

- **Planning**
  Planning upgrades or enhancements to the institution's current infrastructure is essential. Institutions' infrastructures will need to be enhanced over time, therefore plans need to be drawn up looking at long as well as short term goals to allow the infrastructure to continue to evolve, yet at the same time remain a reliable, coherent and sustainable resource. Goals and visions, whether short term or long term, need to be based on the gains to the learner, educator or institution as a whole. In this way, the institution will be able to plan for improvements to its infrastructure being led by educational requirements rather than focussing on perceived technical requirements.
- **Management and support**
  Management and support of the ICT infrastructure is of paramount importance. Users need to be confident that the network will work reliably and consistently allowing them to concentrate on their learning, educating or administration activities. Becta has carried out a considerable amount of work in the field of network management and support by developing and helping institutions to implement the Framework for ICT Technical Support (FITS). Familiarisation and adoption of this scheme of work ought to be considered as a prerequisite to meet the requirements outlined in this document (http://www.becta.org.uk/technicalsupport).

Wording conventions

The following wording conventions apply to the specifications set out in this document:

- The word "***shall***" (italicised and bold) defines a *mandatory* requirement of this specification.
- The word "***should***" (italicised and bold) defines a *highly recommended* but not a mandatory requirement of this specification.
- The word "***may***" (italicised and bold), means that the definition is optional, but is to be considered.

Design prerequisites

It is acknowledged that the majority of institutions will wish to implement the requirements and recommendations in a phased manner. It is important that institutions recognise that alterations to one aspect of their infrastructure can impact upon the entire infrastructure, and that an action plan must be produced to allow the upgrades and replacement of equipment to occur in such a way that disruption to institution functions is minimally disrupted.

Design Criteria

- Institutions ***shall*** conduct a full infrastructure survey prior to major changes to their infrastructure.
- Where major changes are planned an institution ***shall*** produce an action plan outlining the changes to be made to the infrastructure with full consideration of their impact upon the institution.

1 Local Area Networks in institutions

Introduction.

The technical backbone that underpins all aspects of ICT, the institutional network, must be constructed to be coherent, affordable and sustainable. Therefore, this section of the document focuses on implementing and developing a network, using recognised standards, that supports flexible and reliable use of ICT in institutions.

1.1 Wired networks

Wired networks have become the industry standard due to their superior data rates, low-cost and high degree of stability, with wired networks ubiquitous in education as the fundamental technology underlying LANs. Wired networks are therefore to be used as the main network in an institution.

1.1.1 Network topology

The topology of a network describes the physical or logical shape of a network. It is key to the efficient operation of the network, and becomes more important as higher demands are placed upon the network by data intensive applications such as video conferencing. In certain network topologies, if one computer stops working then the network will fail for all computers in that network. In a classroom this would mean that one malfunctioning computer could affect all the other computers' links to the curriculum material located on the curriculum server. Other network topologies could limit the institution's ability to stream different videos concurrently to different computers on the network. With the increasing demands placed on the network from multimedia applications a well designed network is becoming ever more important.

The wired network needs to be constructed in a star or tree configuration (see Fig a.). Star/Tree configurations are scalable and are not affected by the loss of one or more nodes in the network, giving better "uptime".

Every device in the recommended star network is served by a managed switch, which enables multicast (communications between a single sending computer and multiple receiving computers), and provides a more robust model in case of faults. If network segment A has a problem, networks segments B, C and D will still be able to function (See fig a.)

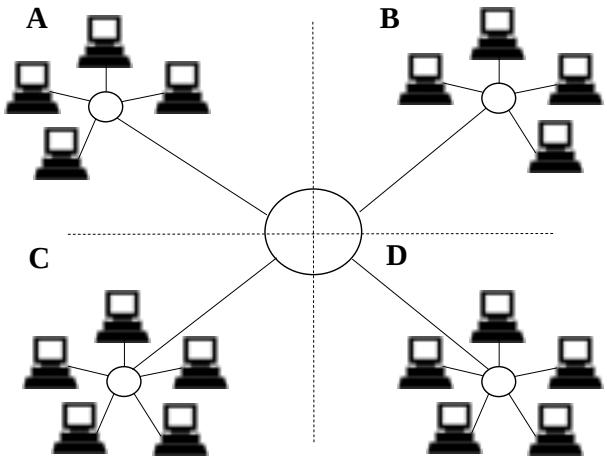

Fig. a: A Star network Topology showing several linked star networks

The Survey of LAN Infrastructure and ICT Equipment in Schools[8] indicates that the vast majority of institutions are using star topology networks, however it is recognised that many of these may be

[8] http://www.becta.org.uk/corporate/publications/documents/BEC4723_LAN_Infrast_A_W.pdf

networks that combine both switches (managed and unmanaged) with hubs. . To ensure the best performance from a star network, hubs need to be upgraded to managed switches.

Design criteria

- Institution networks ***shall*** be of a star/tree design
- Institution networks ***shall*** use managed switches

1.1.2 Ethernet (IEEE 802.3)

There are several types of wired network standards defined under the IEEE[9]'s 802 family of network standards, however there is one set of standards that have become completely dominant in both public and private sectors; those defined by the 802.3[10] standards, also known as Ethernet. The vast majority of new network installations are Ethernet based, and the hardware needed to implement these networks is widely available, sustainable and reliable. The IEEE has ratified several renditions of Ethernet. Typically, the most up to date standard (currently 802.3ae[11] – 10Gb Ethernet over fibre optics) is rarely used due to cost limitations and the practice of giving technology a time to "bed-in". Therefore an 802.3 standard that has been in the market place for sometime is treated by the industry as the most practical up to date standard and equipment made widely available to those standards.

When implementing an institutional network, cost is always going to be a major factor in the choice of equipment. Whilst Gigabit Ethernet is becoming more common, it is still more expensive than Fast Ethernet (Ethernet running at 100Mbs), especially at a network infrastructure level (Gigabit switches currently cost almost double their Fast Ethernet equivalents). It is anticipated, however, that the cost of Gigabit networking will continue to reduce, and the operational life of this equipment will be longer than equivalent Fast Ethernet making it a more sustainable and 'future proofed' resource.

Design criteria

- Institutions ***shall*** implement an Ethernet based wired solution as their primary network.
- Institutions ***shall*** install 802.3ab or 802.3z Ethernet in their backbone, between their servers and key network hardware.
- Institutions ***should*** install 802.3ab or 802.3z Ethernet (Gigabit Ethernet) in new builds or when upgrading their current network.

1.1.3 Cabling

Ethernet is capable of running across three different types of cable: copper twisted pair; fibre optic; and coaxial. Of these, coaxial is used in bus topology networks (see 1.1.1 Network topology) and as such is not appropriate for institutional networks. Both Fibre Optic and Twisted Pair are suitable for Star configured networks and have their own pros and cons:

Category 3 copper twisted pair (Cat3)

- Pros: Inexpensive.
- Cons: Limited to 10Mbps maximum data rate so unsuitable for institutional networks. Maximum 100m run of cable without a repeater (maximum of 4 repeaters).

Category 5 copper twisted pair (Cat5)

- Pros: Less expensive than Cat5e or Cat6. Can run up to 100Mbps data rates.
- Cons: Incompatible with Gigabit Ethernet. Can cause complications with Power over Ethernet. Maximum 100m run of cable without a repeater (maximum of 2 repeaters).

Category 5e copper twisted pair (Cat5e)

- Pros: Less expensive than Cat6. Can cope with a 1Gbps data rate and has been shown to be able to run data at 10Gb. Able to carry Power over Ethernet with no complications. Compatible with 802.3ab.
- Cons: Maximum 100m run of cable without a repeater (maximum of 2 repeaters).

[9] http://www.ieee.org
[10] http://www.ieee802.org/3/
[11] http://www.ieee802.org/3/ae/index.html

Category 6 copper twisted pair (Cat6)

- Pros: Can cope with a 1Gbps data rate. Can implement Power over Ethernet. Is future-proofed for greater speeds and future 802.3 standards. Compatible with 802.3ab.
- Cons: More expensive than Cat5e. Maximum 100m run of cable without a repeater (maximum of 2 repeaters). Due to thickness of cable, there are limits to how tightly it can be routed in bends that might cause routing issues.

Fibre Optic cable

- Pros: Can cope with up to 10Gbps data rate. Future proofed for higher data rates. 2km cable length and greater is possible. Compatible with 802.3z.
- Cons: Can't carry power. Currently, very expensive.

Design criteria

- The network ***shall*** be cabled with fibre optic cable or Cat5e or Cat6 copper cabling.
- Any copper cable ***should*** be rated to at least 350Mhz to ensure data integrity at high data rates.
- Installed cable ***shall*** have the ability to support data rates of up to 1Gbit.
- Where fibre is used for longer spans it ***should*** be single-mode.
- Where single mode fibre is used it ***should*** be 8.3/125 micron fibre.
- Where multimode fibre is used it ***should*** be 50/125 micron fibre.
- Cat3 or Cat5 ***shall*** be replaced with Cat5e or Cat6 or fibre optic cable.

1.1.4 Network Interface Cards

A network interface card (NIC) is the hardware that allows a device to communicate across the network. Some modern devices have this integrated on their motherboard, and others will use a separate expansion card. NICs are rated according to the maximum network data rate that they support, and some cards are able to support more than one data rate. The available rates are 10Mbps, 100Mbps, 1Gbps and 10Gbps.

Design criteria

- Institutions ***shall*** have NICs that support at least 100Mbps in every device connected to the wired network.
- Institutions ***should*** implement 1000Mbps NICs for all new devices connected to the wired network

1.1.5 IP addressing

Public and private addresses.

Public addresses are IP addresses that are defined by the four regional Internet registries -- ARIN, RIPE NCC, LACNIC and APNIC so that any device in the world can communicate with that device as defined by its address. However, with the numbers of devices in use, and the fact that the majority of those devices do not directly connect to a WAN, there are a series of "reserved" addresses for use with devices that do not need a unique identifier. This allows an IP network to run within an institution without that institution needing one public IP address per device. 172.16.*.* through to 172.31.*.*, 192.168.*.* and 10.*.*.* have all been designated as private IP ranges.

Design criteria

- Public IP addresses ***shall*** only be allocated to outward facing devices (normally the institution's router).
- IP addresses ***should*** be allocated by the institution's RBC or LA.

DHCP.

Dynamic Host Configuration Protocol, or DHCP, is a protocol designed to make the administration of IP addresses easier. It allows addresses to be assigned by a DHCP server, which will assign those addresses on a need basis, reusing freed addresses. The DHCP server supports static IP addressing, as well as dynamic allocation and manual address allocation. Static devices, such as servers, printers and network connected learning tools ought to be allocated static addresses that are specified to the DHCP server and kept in an IP range outside DHCP's purview. DHCP runs on ports 67 (Server) and 68 (Client) UDP.

Design criteria

- Institutions ***shall*** use DHCP for IP address management in accordance with any LA, RBC or national addressing scheme.

NAT

Network Address Translation or NAT, (also occasionally known as network masquerading or IP-masquerading) is a technique in which the source and/or destination addresses of IP packets are rewritten as they pass through a router or firewall. It is most commonly used to enable multiple hosts on a private network to access the Internet using a single public IP address. NAT can, however, cause problems for QoS/CoS and video conferencing applications, amongst others, as it adds a layer of complication to routing packets.

Design criteria

- NAT ***should*** be applied at LA level [12]

1.1.6 Wired networks upgrade path

Many institutions will already have a network in place; this network may already meet some or all of the standards laid out in this document, however if it does not, there are a number of options open to the institution. This upgrade path is outlined in the table below.

Current Network	Base Upgrade	Advanced Upgrade
No Network installed.	N/A	Cabled with Cat6 or Fibre Optic cable. Gigabit Ethernet switches installed. Gigabit NICs installed in clients/servers.
10Mbps Network installed	Cable upgraded to Cat6 from Cat3 (Any Cat5e cable may be retained but ***should*** be phased out when possible). 10Mbps or 100Mbps switches (or hubs) replaced by gigabit switches. 10Mbps NICs replaced by 100Mbps NICs in desktops 10Mbps or 100Mbps NICs replaced by Gigabit NICs in Servers	Cable upgraded to Cat6 or Fibre Optic. 10/100Mbps switches replaced with Gigabit Ethernet switches. 10/100Mbps NICs replaced by Gigabit Ethernet NICs
100Mbps Network installed	Cat5e cabling retained (Cat5 shall be phased out when possible). 100Mbps Switches replaced with Gigabit switches 100Mbps NICs retained in desktops. 100Mbps NICs replaced by Gigabit NICs in servers.	Cat5e cable replaced with Cat6 or Fibre Optic cable. 100Mbps switches replaced by Gigabit Ethernet switches. 100Mbps NICs replaced with Gigabit Ethernet NICs.

1.2 Wireless networking

Wireless networking can provide an additional layer of flexibility to enhance traditional wired networks, allowing access to the network from previously inaccessible locations. Using wireless technologies it is relatively inexpensive to add devices to the network and is a comparatively simple task only requiring cabling at the interface between the wired and wireless network. The drawbacks to wireless connectivity are: data rates are normally much slower than conventional wired Fast Ethernet,

[12] It is important that the location of the network edge be examined when choosing how to implement NAT and DHCP, so that duplication of effort can be avoided. The NEN design document (http://www.becta.org.uk/NEN) contains advice on the best implementation of NAT by an LEA in order to ensure that their institutions are able to form a part of the National Education Network.

rendering many current wireless technologies unsuitable for heavy use of high bandwidth applications, such as video; data rates drop as the client moves further from the wireless access point; and it can suffer interference from other devices and frequency congestion, resulting in a drop in data rates and data loss. Whilst the development of wireless networking technologies continues apace, it is not anticipated that this technology will replace the existing wired networks entirely. Therefore, wireless networks need to be seen as giving flexibility to an institution's switched 802.3 standards-based wired network. Wireless security issues are addressed in the section 3.4.2.

Before any institution implements a WLAN a feasibility study and site survey ought to be performed. This will indicate to an institution exactly where wireless networking can be used and how best to enable it to enhance the institution's LAN.

Wireless networks used in institutions as additions to their fixed network infrastructure must conform to the IEEE 802.11a/b/g standards [13]. These are the industry standard wireless specifications, which provide wireless access within appropriate frequency bands.

Standard	Nominal Data Rate	Actual Typical Data Rate	Typical Range	Frequency	Non-overlapping Channels	Comments
802.11b	11Mbps	4-7Mbps	Indoor: 30m Outdoor: 100m	2.4GHz	3	Currently available for use without licence in the UK.
802.11g	54Mbps	18-30Mbps	Indoor: 30m Outdoor: 100m	2.4GHz	3	Currently available for use without licence in the UK An extension of 802.11b. Uses the same encoding technology as 802.11a (OFDM), increasing the data rate. Is backward compatible with 802.11b
802.11a	54Mbps	17-28Mbps	Indoor: 15m Outdoor: 30m	5GHz	8	Currently available for use without licence in the UK.

802.11a is a technology that uses the 5GHz frequency range to achieve declared transfer speeds of up to 54Mbps (typically the actual speeds are closer to 20Mbps), and is able to deploy eight non overlapping channels. In practice, 802.11a is better suited to environments with multiple users using applications with high data throughput. In an education environment this might be a small group using multimedia, digital video, or databases packages.

802.11g also provides a nominal 54Mbps (actual data rates between 10-20 Mbps), but uses the 2.4GHz frequency range, as does the older 802.11b standard, and is only able to support 3 non-overlapping channels.

As the 802.11b standard has been superseded by the faster 802.11g it is not recommended that institutions purchase further 802.11b equipment. 802.11g is backwards compatible with 802.11b making integration relatively easy. Many manufacturers now produce "dual-band" (which can also be referred to as "tri-band") devices that are able to operate using 802.11a/b/g standards as the situation dictates, and these devices, whilst slightly more expensive, can provide an excellent level of flexibility. It is important to note that using an 802.11b device on an 802.11g network will cause the 802.11g devices that share that network to run at a slower speed than an exclusively 802.11g environment.

[13] http://standards.ieee.org/getieee802/802.11.html There are other wireless networking technologies available, but these are not normally designed, or suitable, for use as part of the LAN

Many manufacturers have released proprietary extensions to the 802.11g standard. Often called names such as SuperG or G plus, these technologies provide double data rates, but at the expense of standard 802.11g performance. Consequently it is not recommended that institutions use the expanded data rates that these products can offer, as it can lead to reduced functionality of the base 802.11g network and a lack of compatibility between devices from competing manufacturers.

The next standard expected to be ratified by the IEEE is 802.11n, which will provide higher data rates via wireless. As the standard is yet to be ratified (at the time of writing), it is not recommended that institutions invest in "pre-n" equipment, which will be based on un-ratified, draft standards and constitutes a "best guess" from manufacturers as to the format that 802.11n will take. Implementing this equipment will cause compatibility issues once the standard is ratified and may even cause issues with 802.11g equipment.

Wireless management tools allow network administrators to control, manage and report upon activity across the WLAN, and will simplify the everyday operation of WLANs, ensuring smooth deployment, enhanced security, and maximised network availability, while reducing deployment and management times. They can allow administrators to detect, locate and mitigate rogue access points as well as automatically configuring new additions to the WLAN.

Further explanations of wireless networking technologies are available in Becta's WLAN technical paper[14].

Design criteria

- Wireless networking equipment ***shall*** conform to the IEEE 802.11a/b/g standards.
- New wireless networking equipment ***shall*** conform to IEEE 802.11a or 802.11g standards.
- Wireless networks ***shall*** be secured as set out in section 3.4.2.

1.2.1 Upgrade path

Current Network	Base Upgrade	Advanced Upgrade
No Wireless Network installed.	Install 802.11a or 802.11g compliant access points and Wireless NICs	Dual (Tri) band equipment installed to provide 802.11a/b/g functions Wireless management tool implemented
802.11b equipment installed	Access points upgraded to 802.11b/g equipment New wireless NICs to be 802.11g compliant. Phase out 802.11b equipment when possible.	Access points and wireless NICs upgraded to dual (tri) band equipment Wireless management tool implemented Replace 802.11b equipment with 802.11g compliant equipment
802.11a or 802.11g equipment installed	Access points and wireless NICs retained	Access points and wireless NICs retained Wireless management tool implemented

1.3 Connecting multiple buildings

Connecting all institution buildings to one primary network provides a number of challenges. A number of different factors need to be considered when connecting multiple buildings: the number of networked devices within the building; the distance between the buildings; whether laying of cables is a viable option; and the speed of network required.

[14] Available from http://www.becta.org.uk/technicalpapers

Technology	Pros	Cons
Fast/Gigabit Ethernet over Cat5/6 cable	No change of transport between buildings Fast data rates	100m maximum segment Potential hazard from lightning
Fast/Gigabit Ethernet over fibre optic cable	Large segment length Fast data rates Unaffected by environmental factors	Expensive equipment Requires new cable to be laid
Wireless point to point	No requirement for new cabling Large distances able to be covered	Subject to environmental hazards (e.g. fog for optical connections) Can require line of sight Data rates too slow for more than a few connected devices
Powerline Networking	No requirement for new cabling Straightforward installation	Cannot pass through electrical transformers Slow transfer speeds

Laying cables possible

Fast Ethernet or Gigabit Ethernet cabling can be used, but only if properly shielded in ducting to prevent electrical interference from lightning storms. The maximum length of any single length of Cat5/6 cabling is 100m (and even with a repeater unit this can only be extended to 200m), consequently there may be occasions when this type of cabling is unsuitable, and fibre optic cabling or wireless connections might provide a better option. Optical fibre is fast (speeds of up to 10Gbps are possible), reliable (fibre transmission is unaffected by environmental factors), and has exceedingly large potential ranges (up to 40km using single-mode fibres), which makes it very suitable for connecting multiple buildings in an institution. It is, however, relatively expensive and if there is a problem with the cable then the entire fibre run requires replacing.

Laying cables not possible

Where laying of cables is not possible or favoured there are currently three types of technologies that could be used for connecting multiple buildings, depending on the number of networked devices that a building contains and their use. Point to point wireless connections (which can comply with a number of different standards, including the 802.11 family of standards) can handle distances in excess of 3 miles, and have the added advantage of not requiring any cable to be laid. However, these connections often require that there be line of sight between the transceivers and can be affected by adverse weather conditions. Buildings could be connected using 802.11a/g WLAN technology to bridge to the wired network allowing the wireless segment to function as an integral part of the main network. This option is best used if there are relatively few devices to be networked or device usage/demands are low.

Powerline networking, where data is passed across the conventional building power network using the cables which are already installed to carry mains power, can also be used to connect buildings. This is a very convenient option, as it requires no new cables to be installed. However, data passed onto a power line cannot pass through an electrical transformer without becoming corrupted; therefore if there is a transformer between buildings then power line networking cannot be used. Also, the transmission speeds of a power line network using the de facto Homeplug[15] 1.0 standard are capped at a maximum 14Mbps, which represents a bottleneck when connecting institution network segments. Until the Homeplug Alliance release their Homeplug AV specification this will remain the case.

High speed point-to-point wireless connections come in a number of different types, each using different carriers. Microwave, laser, optical and radio carriers can all be used to transfer data at high rates across distance wirelessly. Each carrier has standards associated with it, and each equipment manufacturer implements a different standard. Until the ratification of the IEEE 802.16e[16] wireless broadband standard (WiMax), it is not anticipated that there will be a single lead standard in this field.

[15] http://www.homeplug.org
[16] http://www.ieee802.org/16/tge/

Institutions must therefore implement an internationally ratified standards-based solution when implementing high-speed wireless links.

Design criteria

- Where device usage is high or in excess of 10 devices are to be networked, cable ***should*** be used wherever possible.
- If distances between buildings is less than 100m:
  - Optical fibre ***should*** be considered.
  - Duct shielded Cat6 cabling or fibre **may** be installed.
- For distances between buildings of 100m to 200m:
  - Optical fibre ***should*** be considered.
  - Duct shielded Cat6 cabling **may** be used in association with a repeater unit.
- For distances between buildings of greater than 200m:
  - Optical fibre ***should*** be used.
- Where device usage are low, or less than 10 devices are to be networked, and cabling is not possible/favoured:
  - 802.11a/g or Powerline technologies **may** be used.
- Where device usage is high or more than 10 devices are to be networked and cabling is not possible/favoured.
  - High bandwidth point to point wireless connections ***should*** be used.

1.3.1 Upgrade path.

Connection Priority	Basic Upgrade	Advanced Upgrade
Cabling possible/favoured and distance less than 100m	100Base-T Cat6 based cabling properly duct shielded 100Mbps (100Base-T) Ethernet managed switch	1000Base-SX fibre Gigabit (1000Base-SX) Fibre switch
Cabling possible/favoured and distance is between 100 and 200m	100Base-T Cat6 based cabling properly duct shielded 100Mbps (100Base-T) Ethernet managed switch 100Mbps (100Base-T)Ethernet repeater	1000Base-SX fibre Gigabit (1000Base-SX) Fibre switch
Cabling possible/favoured and distance is greater than 200m	1000Base-SX fibre Gigabit (1000Base-SX) Fibre switch	1000Base-SX fibre Gigabit (1000Base-SX) Fibre switch
Cabling not possible/favoured	802.11a/g compliant point to point WLAN bridge	100Mbps+ point to point WLAN Bridge

1.4 Network type

Learners, educators and administrators need to be able to electronically store and access their work, teaching materials and administration data wherever they are in the institution. In order to achieve a system where data can be stored and accessed in a secure and reliable manner from all the institution's computers, a dedicated repository (or series of repositories) will be needed where data can be backed up and physical security can also be ensured.

It is required that institutions implement a client/server architecture for their main wired network. It is for the institution to decide whether this is implemented via a fat client or thin client approach. A client/server architecture stores data centrally providing accessibility of data, central control of resources and facilitating data integrity assurances.

It is required that learner and administration data be available from any device in the institution. This can be achieved by having the data held on a single integrated logical network, rather than separate networks. The use of VLANs and subnets to combine separate physical networks and allow user-based access to the different data types provides a reduction in the support overhead and allows staff to access admin functions from the same terminal that they use to access learning content.

Design criteria

- Institutions ***shall*** use a client/server network architecture.
- Institutions ***shall*** implement a repository with functionality for allowing mirroring of data and redundancy of physical media.
- Data ***shall*** be backed up at intervals as defined in Section 3.3.2.
- A secure link ***shall*** be provided to the central repository.

1.4.1 Fat Client networks

Characteristics of a client/server network

- Central Server containing data is readily accessible by all users.
- Data is easily managed with central backups leading to less likelihood of data loss.
- A unified user policy can control access to files and resources.
- A reduced overhead on client devices.

An institution's centralised data repository needs to have certain technical requirements fulfilled. It must reside on the backbone of the network, ideally a gigabit connection[17], in order to provide sufficient network bandwidth. This backbone must be switched to provide the best possible routing of data, and ought to have at least a Class of Service function (See section 1.5 Prioritising traffic) included to ensure prioritisation of data across the network. The server ought to also have a RAID function on its hard drive array, allowing mirroring of data, and redundancy of physical media to prevent data loss in the event of a disk fault. Needless to say, full backups ought to be taken of all user data at daily, weekly and monthly intervals, and the backups stored in a separate building to the server as well. In addition it is recommended that institutions make provision for total server failure and have a backup server ready to be switched to with a mirror of all data, in the event of the loss of the main server.

Design criteria

- The centralised data repository ***shall*** reside on the network backbone unless it is held outside the institution.
- Data rates between the central repository and the institution ***should*** be no slower than 100Mbps.
- Where data rates between the central repository and the institution are lower than 100Mbps, then a caching repository ***should*** be implemented at the institution.

1.4.2 Thin Client networking

Characteristics of a Thin Client network

- Client/server network architecture.
- Majority of processing carried out by the servers.
- Centralised management functions for security, anti-virus, patching, etc.
- Thin client workstations require less processing power than fat clients.
- Applications controlled centrally by the server user policy.

"Thin client" networks, where most of the processing of data occurs on the server, have a number of advantages over the more common "fat client", with cheaper terminals, central application control, and enhanced security. However, there are also clear disadvantages to such an implementation: thin clients are usually less able to deal with complex video and audio demands; and specialised thin client terminals lack the flexibility offered by fat client machines.

The servers in a typical thin client network require sufficient processing power and memory. With all the clients on the network demanding that their processing be done on the server, the specifications of the servers (and thus their cost) may need to be higher than the servers in a fat client environment. However the extra cost of these servers over a fat client solution can be offset by relatively cheaper

[17] Whilst gigabit Ethernet is specified for use in the network backbone, there are certain situations in which the repository is held outside the institution. In these cases, it is unrealistic to expect this to be served by a gigabit link.

client machines. The reliance upon these servers is not seen as a major disadvantage, as it is usual that a fat client implementation will be equally reliant upon the network servers – the loss of a server with certain fat client operating systems can render those fat clients useless.

Thin client solutions do often require more servers than fat client architectures. As all the processing for a thin client implementation is done on the servers, there are limits to the number of concurrent users that a thin client server can support. It is vital that institutions that implement a thin client solution consider the number of users that may use the system concurrently and ensure that their servers are sufficient to support this.

A properly implemented thin client will use little more bandwidth than a properly implemented fat client architecture, however there is an increase in the number of network packets generated by a thin client solution. As these packets are small and frequent, it is vital that the network is built around hardware that can process these large numbers of packets in a timely and accurate manner. Wireless networking makes available lower bandwidth, and is often subject to greater packet loss than wired networking, and therefore performance may suffer if a thin client solution is implemented over a WLAN.

Thin client machines can come in two main varieties; true thin clients and converted clients. True thin clients are specialist machines designed specifically to run thin client solutions, they often have no hard drive and are built around solid state technologies. This makes them smaller, lighter and harder to break (as well as cheaper) than regular PCs, but does mean that if an institution ever changes from a thin client architecture to a fat client architecture then these machines will be useless. It is also not possible to install specialist software onto these machines as they tend to lack the hard drive capacity to run software independent of the thin client server. Converted clients are those PCs that are bought as full client machines that are then reconfigured to act as thin clients. This provides the advantage of longevity of active lifespan, as older machines that are unable to run modern versions of operating systems can be converted to thin clients and continue to provide useful functions within the institution.

These thin client desktops will also lack much processing power of their own and so are less flexible, with the application set being dictated by the central server rather than having the ability to load specialist software onto individual devices, as is provided by a fat client network. Furthermore, it is not advisable to configure laptops as thin clients if they are required for use off the network. Any laptop configured in such a manner is likely to be unable to function when removed from the institution's network, as it will no longer have a connection to the server from which its applications run. Thus it is likely that an institution running a thin client network will wish to have fat client laptops for use offline, which then run a "terminal emulation" program to act as a thin client whilst wired to the network. Whilst this is entirely possible, it can lead to user confusion as the user may require a different login procedure depending on whether the device is connected to the network or not, and therefore care must be taken to ensure that users understand the logon procedures required.

If these issues can be addressed and overcome, then thin client networks do offer a very secure network, with the ability to control user access and rights much more easily than by using a fat client system. Central application control means that application upgrades and enhancements can be applied quickly and easily across an entire institution, making the support overhead of applications on a thin client network much less. There is also a reduced cost to the institution as far as the desktop devices are concerned, as the processing functions are carried out at the server.

Thin client technology is an area of growth within the ICT industry, with many suppliers and manufacturers arguing that it is the way forward for Client/Server computing, especially in high user, low budget environments such as educational institutions. However, challenges remain to be overcome before this technology can provide full functionality as is required by modern institutions. Consequently, it is strongly recommended that an institution study very closely their functional requirements before deciding upon a thin client network as their main wired network; and most institutions will wish to seek assistance from their networking partners before committing to thin client networking.

Design criteria

- Full thin client implementations ***shall*** be capable of providing all apps and services as defined in chapter 2.
- Where thin client implementations are unable to provide all apps and services as per chapter 2, then it ***shall*** only be used in conjunction with a fat client implementation.

1.4.3 Peer-to-Peer networks

Peer-to-Peer networking involves taking a number of devices and connecting them together in a small self-contained cluster, with no connection to a large network or server. These networks are often used on an ad-hoc basis, and wireless networking for small groups of learners and educators who need to set up a small dynamic network of their own is especially suited to this kind of network. P2P networking may be used in institutions, when appropriate (small clusters of P2P wireless devices can be useful for group working), but ought to only be used to in support of a client/server environment and not to replace it.[18]

There are a few issues that it is important any institution remain aware of when using peer-to-peer networks. If a DHCP server is used to allocate IP addresses when on the normal institutional network, then (unless it is included in the P2P network) the P2P devices will be unable to retrieve an IP address. This ought to be no problem as long as this is taken into account when the devices are initially configured. Any data saved whilst using the network will have to be saved to one of the client devices, as no server is available. This can lead to a lack of back-ups being taken, or to version conflicts with files saved on the server. Also, P2P networks will tend not to have the same security set ups as permanent “non ad-hoc” LANs, this can lead to security concerns, especially when the network is wireless.

Design criteria

- Institutions using peer-to-peer networks ***shall*** configure devices so that devices gain static or OS defined IP address if/when DHCP fails
- Institutions using peer-to-peer networks ***should*** ensure any data is synchronised with main network on a daily basis

1.4.4 Client/Server Network Design

There are a number of options for institutions when implementing these architectures, dependant upon their circumstance and ties to other organisations.

Standalone institution.
This institution would require its own data repository, linked to its gigabit network backbone. The institution will require appropriate hardware with enough space for its data. The institution will also need to monitor space on, and availability of the repository; as well as ensuring that the data is backed up and stored appropriately. (Advice on the operational management of the repository is currently being produced by Becta.)

RBC/LA/Managed Service Provider maintained repository.
It is possible for a institution to have their central repository provided, maintained and configured by their RBC, managed service provider or LA. The advantages to such a configuration are that it allows the data repository to be aggregated between a number of institutions, allowing the pooling of resources between the served institutions and a central single support structure put in place to maintain the server and its access. However, it does also leave a single point of vulnerability to outage for all the institutions sharing the server resource, and the remote nature of the hosting organisation (LA) can mean that maintenance and development issues can take longer to resolve. There can also be an issue with the speed of connection between the repository and the institution due to connectivity limitations. 100Mbps connections as a minimum are required, however this will often not be possible between institutions and the LA/RBC, and so where there is a lower rated connection, institutions ought to implement a repository on their LAN which caches day-to-day work and then replicates it to the LA/RBC repository every evening. This caching repository ought to reside on the network backbone.

[18] It is worthy of note that this form of networking is distinct from the “Peer-to-Peer networks” used for file sharing on the internet, as popularised by Napster.

Paired/Clustered Institutions.
It is also possible for small institutions to share space on a server with larger institutions who own and control the repository, either singly or in "clusters" of institutions. Thus a small primary school, for which a dedicated server is an expensive resource used to less than its capacity, could have dedicated space on the server of a larger organisation, such as a secondary school. Access to the server and its information could then be accessed through a policy of trust between the two (or more) institutions (such as trusted domains). This would allow the primary school access to a dedicated repository without the need for investment in its own server resource. The disadvantage to this, as with the server held at an RBC/LA/MSP, is that the primary school has a great deal less control over the server, and consequently their data, than they would if it was their own dedicated resource.

1.4.5 Virtual Local Area Networks (VLANs)

Virtual LANs in a switched network are a logical collection of users and devices grouped to form a single broadcast domain. This grouping of users/devices allows routing of data traffic based on group policies, giving enhanced control of security, traffic density and user access. However, information sent between devices on different VLANs must be routed by a VLAN capable switch, to ensure that the data reaches the correct destination.

Unlike typical LANs, which are limited by geography, VLANs create "virtual" networks that can span buildings, LAs, or even collections of institutions globally. VLANs allow the network administrator to create logical groupings based on an institution's requirements, not arbitrary physical locations.

For all of these methods, VLAN assignment requires the switch to classify traffic and match it to VLAN definition policies quickly and accurately. The switch ought to be able to classify traffic based on its physical port, address (MAC/IP or combination), protocol type, multicast address, user ID and password, or a combination of these criteria.

Today the most common VLAN standard is the IEEE 802.1Q[19] specification, which most vendors support. IEEE 802.1p[20] (see 1.5.1 Class of Service (CoS)) works in conjunction with 802.1Q and allows for the prioritisation of VLAN traffic. Although most switch vendors offer some type of integrated VLANs, the services available vary.

Design criteria

- Institutions ***shall*** ensure that all new switches joined to the network are 802.1Q compliant (see 1.5.1 Class of Service (CoS))
- Institutions ***should*** replace older switches and hubs with managed 802.1Q compliant switches.

1.5 Prioritising traffic

In every institution's network there are likely to be certain applications that need preferential access to the institution's network in order to gain satisfactory performance. For example, video conferencing applications will need the network to handle their data as a matter of priority. If this data is not prioritised then a breakdown in audio and visual quality could occur. If this sort of use of applications is echoed in several places in the institution then high demands are placed on the network. Without a system in place to control how the network deals with these multiple high level demands and gives priority to certain applications or parts of the network, the experience for the student and indeed staff could become a very frustrating and unsatisfactory one.

1.5.1 Class of Service (CoS)

Class of Service (CoS) is a way of managing traffic in a network by grouping similar types of traffic (for example, email, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority. Unlike Quality of Service (QoS) traffic management,

[19] http://www.ieee802.org/1/pages/802.1Q.html
[20] http://www.ieee802.org/1/pages/802.1D.html

Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." On the other hand; CoS technology is simpler to manage and more scalable as a network grows in structure and traffic volume.

There are three main CoS technologies:
802.1p Layer 2 Tagging
- Pro – provides an eight level prioritisation scheme that constitutes “best effort” CoS.
- Pro – support is implemented in most modern operating systems.
- Con – layer 2 is application neutral so this scheme requires user configuration.

Type of Service (ToS)
- Pro – efficient prioritisation of packets by header performed by the router.
- Pro – in conjunction with IP preference is widely supported.
- Con – being phased out in favour of DSCP.

Differentiated Services (DiffServ) with DSCP[21]
- Pro – Fast becoming the industry standard.
- Pro – Uses DSCP header prioritisation.
- Con – Some older network devices may not support this protocol.

802.1p Layer 2 Tagging and ToS make use of three bits in the layer 2 packet header that can be used to specify priority. Since three bits does not allow for much sophistication in managing traffic, a new protocol, Differentiated Services (DS or DiffServ), has been developed in draft form by an IETF Working Group. Differentiated Services uses a different approach to managing packets than simple priority labelling. It uses an indication of how a given packet is to be forwarded, known as the Per Hop Behaviour (PHB). The PHB describes a particular service level in terms of bandwidth, queuing theory, and dropping (discarding the packet) decisions and all of this information is stored in the packet header using the DSCP protocol.

Design criteria
- Institutions using CoS ***shall*** detail a table of priorities so that their CoS policy is easily understood.
- Classification of applications ***should*** be limited to a select few applications so traffic priority can be provided with clearly discernible results.
- Institutions ***should*** implement Diffserv with DSCP as their first choice CoS strategy.

1.5.2 Quality of Service

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics to the network traffic that requires this in order to provide a defined level of service. Also important is making sure that providing priority for one or more flows does not make other flows fail. QoS technologies provide the elemental building blocks that will be used for future implementations of networks in education. Quality of Service is needed to ensure that time sensitive IP applications such as video conferencing (VC), Voice over IP (VoIP), streaming media and multicast can be delivered to a high quality over an institution’s network.

To be effective, QoS must be implemented on an end-to-end basis across each network hop and in each active component i.e. router and switch along the data path from the sender to the receiver, which in a National Education Network (NEN) domain means the local institution, Aggregation areas, LAs, RBCs and the SuperJanet backbone. NEN recommendations are that Service Level Specifications (SLS) and Agreements are established covering all the domains in order to achieve

[21] Many QoS implementations are likely to be built on the foundations laid by Diffserv using DSCP, and therefore it is probable that institutions will benefit from a “head start” towards QoS as they will have this implemented for CoS (see above).

end-to-end operation. The establishment of consistent end-to-end QoS support will be greatly simplified if identical SLS can be used throughout the domains.

Design criteria

- Institutions ***shall*** consult with their LA, RBC, and service providers to ensure that QoS is implemented in a manner conducive to end-to-end delivery.
- Institutions ***shall*** ensure that SLS are in place if they are implementing QoS.

1.6 Flexible access

To enable flexible working away from the institution, curriculum and administration data needs to be accessible by authorised users from a range of places although institutions need to decide the level and granularity made available for different groups of individuals. For example, educators need to access teaching materials, learners' work areas and administration data from the institution or from home. Learners will need to access their work area from home and will most likely need to have access to relevant institution notices and information. Secure remote access to relevant administration data needs to be available away from the institution.

1.6.1 Remote access

Remote access has a multitude of potential solutions, some of which have associated standards. Data can be made available via a web interface accessible across the internet, where users access a web interface from the remote site which then gives access to specified resources. A "dial-in" facility can be provided for learners and educators, where the user uses a modem to dial into the network and gain access to data that way. Alternatively, an institution could implement a Virtual Private Network (VPN) allowing users secured access to the network over the internet as if that user was logging onto the network directly. Most of these VPN standards are implemented in proprietary solutions, with layers of "closed" code enfolding the open standards. This makes it very hard for institutions to implement a purely standards based solution for remote access.

It is vital that institutions take into account the security issues surrounding remote access. As an external facing entrance into the institution LAN, any remote access solution has some potential to be misused by malicious individuals. However, as long as commensurate attention is paid to the security of the system, the benefits to learners and educators far outweigh the risks.

If institutions wish to implement remote access now, then it is important that institutions recognise the accessibility issues around these solutions and institute a policy that addresses these issues.

Becta is engaged in ongoing work with regard to remote access. Due to the complicated nature of the issues surrounding the area, and the lack of any clear lead standards, it is advised that institutions consider whether it is currently appropriate for them to implement a remote access solution. For those institutions that do wish to do so, the following offers some advice:

- **Web interfaces**

Remote access can be provided by a web interface, allowing learners and staff to access their data via a web front end. Users can then access this data by connecting to the institution web interface via a browser from their home web connection. The standards that apply to this are HTML, XML, PHP, S-HTTP and SSL.

  - Pro – access to data is relatively straightforward for the user, needing only to "log-in" to a website.
  - Pro – a custom front end can be designed, allowing the institution complete control over their user's remote access experience.
  - Pro – some learning platforms may include this functionality as standard.
  - Con – requires the user to have internet access from their remote site.
  - Con – remote connection is subject to the current internet conditions, less bandwidth makes web interfaces unsuitable for remote access to data intensive applications.
  - Con – can be subject to unauthorised connection attempts as interface is publicly visible.

Design criteria

- Institutions ***shall*** give due consideration to implementing web interfaces for RAS, and ***should*** refer to Becta's ongoing work in this area.
- Institutions using web interfaces ***shall*** use SSL and/or S-HTTP to secure their web interface.

- **Dial-in**

It is possible for remote users to be provided with a dial-in account which they can access over a modem. The user will then connect this modem to a telephone line and dial-in to the institution servers, connecting directly to the network. The primary standard protocol in this area is PPP. Modems are, however, not a future-proofed technology and therefore are not recommended as a lasting remote access solution.

  - Pro – the modem creates a device to device secure connection with the server.
  - Pro – connection is dedicated and so provides all bandwidth to the user.
  - Pro –can provide direct access to the network, allowing the user access to resources as if they were in the office.
  - Con – modems limited to low bandwidth.
  - Con – can be complicated to administer and for the user.
  - Con – one modem needed per concurrent user.

Design criteria

- Institutions ***shall*** not use dial-in solutions as their primary method of remote access.

- **VPN**

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures. There are a number of standards that apply to VPN including MPLS, IPSec, and TLS.

  - Pro – allows a high degree of management over access with comprehensive user access policies and "virtual" seamless network access.
  - Pro – uses existing internet access to connect to the institution's network.
  - Pro – secure and invisible to the public.
  - Con – requires client software to be loaded on the user's device and often will require additional hardware per user (VPN dongles, Smartcards, etc).
  - Con – can be complicated for the user and can require technical support to be provided by the institution to home users.
  - Con – not easily affordable and therefore difficult to sustain as additional capacity is added.

Design criteria

- Institutions ***shall*** only implement a VPN solution if they are able to sustain support for the users as the user bases increases.
- Any VPN solutions implemented by institutions ***shall*** be based around internationally ratified standards for communication and security.

1.6.2 Synchronisation

As an addition to remote access services, synchronisation provides extra functionality and flexibility to learners and educators. Synchronisation is where the user's data is replicated from a repository-contained copy to a local copy held on a portable device. Thus an educator with a laptop can hold mirror images of their documents on both the network repository and their laptop, working on the laptop copy when disconnected from the network and the network copy when connected. Changes from the repository are synchronised with the device and vice-versa at appropriate intervals keeping a relatively up-to-date copy as a mirror image. This improves the accessibility of the data, and allows data to be carried with the user outside of the institution's network.

Care must be taken, of course, with the security of data, and it is important to implement appropriate access controls to ensure confidentiality, integrity and availability of information on both the network and the portable device. More information on this can be found in section 3.5 Internet and remote access security.

Design criteria

- Institutions ***should*** enable synchronisation between appropriate network data and portable devices.

2 Services and applications in institutions

Introduction

Whilst there are obstacles to be overcome in all areas of ICT resources to achieve a complete standards-based approach, there are clear and unique problems when faced with many ICT applications and information services. Applications are frequently designed to work with particular hardware, operating systems or proprietary file formats – often due to the costs of developing and verifying that a product will work on multiple platforms and the additional cost of implementing multiple platform support.

Whilst Becta recognises that applications differ in terms of reliability, functionality or additional features, the main attempt here is to provide a framework of standards that will encourage a level of ICT interoperability that has currently not been achieved.

2.1 Standards for applications used in institutions

To enable educators and learners to have a fulfilling and useful ICT experience it is necessary for them to have access to relevant applications, both administrative and pedagogical. Ensuring each institution makes efficient use of ICT could lead to a reduction in administrative burden, improved communications and an enhanced learning experience by allowing greater personalisation, assessment and continuity of learning. Although the needs of each individual user and institution will differ, a basic core set of applications needs to be made available to all, allowing manipulation of text, images (including video), tables and sounds.

Design criteria

- Pedagogical and administrative applications ***shall*** support open standards that allow the import and export of data in a range of commonly used formats that are independent of a particular platform.
- All educational applications ***shall*** provide an interface that is designed or can be tailored to suit the age and ability of the learners.
- Documents and data which are intended potentially to have a long lifetime ***should*** **not** be solely saved to proprietary file formats.
- Where only proprietary standards are available, strategies ***should*** be provided for migrating to open formats if and when they become available.
- Applications used in institutions ***should*** be designed for network installation.

2.2 Standards for office productivity applications

Office Productivity applications provide text, spreadsheet, database and presentation slide viewing and editing. There is a vast array of these types of applications, which are often packaged together as an ‘office suite’. Many of the formats that applications save data to are proprietary, with some being considered to be de facto standards. Any office application used by institutions must be able to be saved to (and so viewed by others) using a commonly agreed format that ensures an institution is not locked into using specific software. The main aim is for all office based applications to provide functionality to meet the specifications described here (whether licensed software, open source or unlicensed freeware) and thus many application providers could supply the educational institution ICT market.

The formats included here are set out as a minimum specification to guide institutions to use applications that can write to commonly understood and open standards, as far as possible, to help ensure interoperability.

2.2.1 Text document applications

Design criteria

- Text document applications used in institutions ***shall*** provide the functionality to create, edit, save and print documents in open standard file formats.

Text documents	Plain text as (.txt) files **or** Plain/Formatted text as Rich Text Format (.rtf) files **or** Plain/Formatted text as OpenDocument (.odt) format

2.2.2 Spreadsheet applications

Design criteria

- Spreadsheet applications used in institutions ***shall*** provide the functionality to create, edit, save and print spreadsheet files in open standards file formats.

Spreadsheet documents	Comma Separated Variable (.csv) format **or** OpenDocument (.ods) format

2.2.3 Database applications

Design criteria

- Database applications used in institutions ***shall*** provide the functionality to create, edit, save and print database files in open standards file formats.

Database documents	Comma Separated Variable (.csv) format **or** OpenDocument (.odb) format

2.2.4 Presentation applications[22]

Design criteria

- Presentation applications used in institutions ***shall*** provide the functionality to create, edit, save and print presentation files in open standards file formats.

Presentation files	Hypertext documents (.html) files **or** OpenDocument (.odp) format **or** Interactive audiovisual presentations as Synchronized Multimedia Integration Language (SMIL) format[23]

2.3 Standards for accessing web based content

Hypertext (HTML) based content is used extensively in institutions by learners, educators and administrators. In order to ensure that content can be accessed by using any browser, content must be displayed in a consistent and safe manner.

Design criteria

- Browsers used in institutions ***shall*** be able to display websites using W3C standards.
- Browsers used in institutions ***shall*** allow the installation and use of third party plug-ins.
- Institutions ***shall*** use a content filtering system that ***should*** be managed by LAs/RBCs in discussion with institutions.
- Filtering solutions ***should*** include the use of traffic logs, the display of an onscreen message indicating a site has been blocked, the ability to block sites, and where appropriate, in accordance with user policies, to unblock particular sites.
- Internet access ***should*** be via a Becta Accredited ISP[24] or an ISP that provides the same or similar level of service.

2.4 Standards for creating web based content

Internal and external facing web pages created by or for an institution must be written using W3C standards and be accessible to all users. Liability under disability discrimination laws can be minimised by implementing best practice in web accessibility in line with W3C WAI guidelines. The

[22] The file formats outlined here are intended for desktop office applications. Other display devices, such as Interactive Whiteboards, currently use further file formats which are outside the current scope of this document
[23] http://www.w3.org/AudioVideo/
[24] http://ispsafety.ngfl.gov.uk

guidelines are intended for all web content developers (page authors and site designers) to promote accessibility.

Becta has produced a comprehensive guide to website accessibility, covering basic concepts through to detailed, practical guidance about how to assess and ensure that a website is accessible. This guide is of interest to anyone involved in designing, developing, managing or maintaining websites. It is also important that those involved in designing and creating resources which are delivered through websites also take account of this guidance. “Understanding and implementing website accessibility” can be downloaded from http://www.becta.org.uk/industry/advice/advice.cfm?id=4360.

Design criteria

- Institution domain names ***shall*** be in the format ‘*school*.*area*.sch.uk’[25]
- Website content produced by or for institutions ***shall*** be written using W3C standards (such as HTML v4.01, XHTML v1.0, CSS, XML or XSLT).
- All institution websites ***should*** conform to level 'Double-A' standard, as defined in the Web Accessibility Initiative (WAI - http://www.w3.org/wai) Web Content Accessibility Guidelines.

2.5 Standards for multimedia

It is necessary for open standards to be used that will allow for images and sounds to be accessed, produced and edited on a range of different platforms. The formats mentioned here are set out as a minimum specification to guide institutions to use applications that can write to commonly understood and open standards, as far as possible to, help ensure interoperability.

Design criteria

- Proprietary file formats ***should*** be saved to only when an application is freely available for all workstation platforms via web download.

2.5.1 Graphical/still images

Images and graphics need to be accessible across different platforms and from a wide array of applications. This is an area where open standards are widely used.

Design criteria

- Institutions ***shall*** provide applications with the functionality to create, edit, save and print still image files in open standards file formats.

Lossless images	Tag Image File (.tif) format
Photographic storage (if some information loss may be tolerated)	Joint Photographic Experts Group/ISO 10918 (.jpg) format
Line drawings	Graphics Interchange Format (.gif) **or** Portable Network Graphics (.png) format
Highly compressed images	Enhanced Compressed Wavelet (.ecw)

2.5.2 Audio/video specifications

There are many widely used formats for streaming audio and video, and media players that accept these formats are readily available for free and for most platforms.

Design criteria

- Media players used in institutions ***should*** support at least MPEG layer 3 (.mp3) or Ogg Vorbis (.ogg) for audio representation and MPEG layer 1 (.mpg) for coding moving pictures and associated audio.

[25] See http://www.nominet.org.uk/SecondLevelDomains/AboutSecondLevelDomains/schuk/schuk.html

Video files	Moving Picture Experts Group/ MPEG-1/ISO 11172 (.mpg) files
Audio files	MPEG layer 3 (.mp3) format **or** Ogg Vorbis (.ogg) format

2.5.3 Animation

Open standard formats are rarely used for computer animations; however, many have been produced in formats that can be displayed in web browsers natively or via plug-ins or in other freely available applications.

Design criteria

- Animations developed by or for institutions ***should*** be saved and viewed in a freely available format.

Animation	Macromedia Flash (.swf) **or** Apple Quicktime (.avi, .mov, .qt)

2.5.4 Vector graphics

Vector graphics are images stored and displayed in terms of vectors rather than points. They are used when it is necessary to scale images and typically have a smaller file size than bitmapped graphics, such as GIF and JPEG files. Vector graphics can also be used in complex animation.

Design criteria

- Vector graphics developed by or for institutions ***shall*** be saved in open standard file formats.

Vector Graphics	Scalable Vector Graphics (.svg) format **or** Vector Markup Language (.vml) format

2.6 Learning platforms

'Learning platform' is a generic term covering a variety of different products, all of which support online learning in some way and includes delivery via intranets, via the internet and third party hosting. Learning platform capabilities can vary from systems that provide bespoke learning content or access to third party content only, to systems which provide communications, assessment, tracking and MIS interoperability[26] facilities.

To raise levels of interoperability between learning, assessment and information management systems in institutions, and to inform the investment decisions taken by institutions purchasing these systems, Becta is working to develop a functional specification for Learning Platforms that will be published in March 2006. To inform this work, Becta is liaising with stakeholders and has established a Stakeholder Group (for more information e-mail lstsg@becta.org.uk).

A number of ongoing initiatives are investigating standards and specifications for learning technology, such as IMS (http://www.imsproject.org/), and UK LeaP which is based on aspects of the IMS global initiative. The specifications that these bodies are producing are converging and Becta is investigating these to determine the most suitable of the emerging standards. Until this investigation is complete, educational projects are advised to implement the following design criteria; however, institutions are strongly encouraged to wait for Becta's Learning Platform functional specification to be published before purchasing a Learning Platform.

Design criteria

- Learning platforms that are accessible using web interfaces ***shall*** use SSL and/or S-HTTP to secure their web interface.
- The IEEE Standard for Learning Object Metadata ***should*** be used to describe learning materials.

[26] Becta is currently reviewing Management Information Systems

- The IMS Question and Test Interoperability Specification ***should*** be used to write and describe assessment materials (questions or tests).
- Becta's Packaging and Publishing Learning Objects: Best Practice Guidelines[27] ***should*** be followed for the description, structure, and location of online learning materials.
- The IMS Learner Information Packaging Specification ***should*** be used when developing Learner Information systems.
- The AccessForAll Meta-data (AccMD) specification ***should*** be used to identify resources that match a user's stated preferences or needs. These preferences or needs ***should*** be declared using the IMS Learner Information Package Accessibility for LIP specification.

2.7 Communications

Communications software relies heavily on open standards in order to facilitate intra- and inter-institution communication. Whilst many products on the market claim to be interoperable, institutions need to ensure that any purchased products use recognised open standards.

Design criteria

- Institutions ***shall*** ensure that all communications software purchased or developed for the institution uses recognised open standards.

2.7.1 Video conferencing

At its simplest, a video conferencing solution can be a webcam enabled PC allowing one user to talk to and view another user. More advanced solutions enable whole class conferencing, including multipoint conferencing where three or more clients can collaborate in the same conference.

The UK Government's e-Government Interoperability Framework (e-GIF)[28] makes recommendations with respect to the adoption of ratified IP conferencing standards. These include the H.323 standard, for the assembly of audio, video, data and control. Unfortunately, not all H.323 video conferencing equipment is compatible with another manufacturer's; so it is important that institutions liaise with their RBC or LA before purchasing H.323 video conferencing equipment.

Some regional networks are not designed to allow video conferencing directly between endpoints within the region. H.323 signals will be routed around the region's firewall, so it will be necessary to acquire an external IP address mapped to an internal address that will be used exclusively for video conferencing. There are two options to achieve this: an H.323 Proxy, or an H.323-aware Firewall/NAT device. (See section 1.1.5 for more about NAT). In order to minimise security issues, technical support with videoconferencing network problems, such as those caused by firewalls, must be sought from RBCs, Local Authorities or their approved support centres.

Unless using a dedicated link for video conferencing, it can have an adverse effect on an institution's network, so for a satisfactory performance, a system needs to be in place to control how the network deals with high level demands and to determine network priority. Details of how to implement Class of Service (CoS) and Quality of Service (QoS) can be found in section 1.5.

Information for the successful deployment of a reliable video conferencing service of a consistently good quality across the educational network can be found at http://www.becta.org.uk/nen.

Design criteria

- Institutions ***shall*** consult with their RBC or LA before purchasing H.323 video conferencing equipment.
- Institutions ***shall*** use an H.323-aware Firewall/NAT device or H.323 Proxy (this ***may*** be at the LA or RBC level).
- Institutions ***shall*** register with the Janet Videoconferencing Service (JVCS)[29].
- Institution ***shall*** use the National Education Network for H.323 video conferencing.

[27] http://www.becta.org.uk/page_documents/industry/content_packaging.pdf
[28] http://www.govtalk.gov.uk/schemasstandards/egif.asp
[29] Janet Videoconferencing Service – http://www.jvcs.video.ja.net/

- Institutions ***shall*** arrange Quality Assurance Assessments via JVCS for all room-based video conferencing endpoints.
- Institution H.323 endpoints ***shall*** only accept external calls (those originating from outside of their RBC) from JVCS.
- Technical support with videoconferencing network problems, such as those caused by firewalls, ***shall*** be sought from RBCs, Local Authorities or their approved support centres.

2.7.2 VoIP

H.323 and Session Initiation Protocol (SIP) are the two main standards or proposed standards for VoIP. Many of the networking issues and technologies of VoIP are the same as for video conferencing if using H.323, so the same design criteria apply. SIP is an IETF proposed standard for setting up sessions between one or more clients. It also has a problem with NAT firewall traversal; however, many new firewall products now recognise and pass SIP traffic.

Not all VoIP equipment is interoperable with assistive technologies; therefore care must be taken to ensure that a chosen VoIP solution does not prove a communications barrier for any user.

Design criteria

- Institutions ***shall*** consult with their LA/RBC before purchasing VoIP solutions.
- If replacing existing PBX systems then institutions ***should*** implement VoIP solutions
- H.323 and SIP systems ***may*** need to be configured to traverse firewalls.

2.7.3 Email service

Institutions can choose a POP3 or IMAP email solution. A POP3 (Post Office Protocol) email server receives email and sends the entire message upon a client's request. Once received, the message is no longer stored on the server unless specifically instructed to keep a copy. POP3 is suitable for most remote mailbox access requirements. An IMAP (Internet Message Access Protocol) email server sends a copy to the client computer rather than sending the entire email.

Design criteria

- Email products used in institutions ***shall*** support interfaces that conform to SMTP/MIME for message transfer
- Email products used in institutions ***shall*** as a minimum conform to POP3 for remote mailbox access
- Where additional mail facilities are required, email products that provide advanced mail access facilities ***shall*** conform to IMAP for remote mailbox access
- Mailbox access via a web browser ***shall*** use HTTPS or secure VPN
- Institutions ***shall*** use an email filtering system that ***should*** be managed by LAs/RBCs in discussion with institutions.
- Filtering ***should*** be able to be refined at an institutional level.
- Internet access ***should*** be via a Becta Accredited ISP[30] or an ISP that provides the same or similar level of service.

2.8 Access to content

Effective data management, whether administrative or pedagogical, is essential for an efficient and useful ICT network. Allowing data to be shared reduces the risks that arise with storing multiple copies of similar data and allows institutions to take advantage of collaborative technologies[31]. Ensuring administrative data is well managed, accessible and stored in an open format means that information is shared effectively, timely and efficiently, both internally and with authorised partners, such as LAs.

All content that is accessible in or from an institution must be accessible to all entitled users, whether stored on CD-ROMs, virtual CD servers, network servers or any other media.

[30] http://ispsafety.ngfl.gov.uk
[31] As with all aspects of data use, institutions shall adhere to the Data Protection Act

Design criteria

- Where users will not necessarily have access to the same computer at all times, IMS ACCLIP ***should*** be used to facilitate transferable user customisable interfaces.

2.8.1 Caching and Content Delivery

Caches store temporary copies of learning objects and are designed primarily to improve the accessibility and availability of this type of data to end users. Caching optimises the usage of available bandwidth by allowing users to access a single locally stored copy of the content many times rather than repeatedly requesting the same content from the original source.

Design criteria

- Institutions ***should*** use a caching system and this ***shall*** be as described in Becta's Caching & Content Pre-positioning Technical Paper[32].
- Frequently accessed media rich, static content ***should*** be located as close as possible to the users, such as in the institution.
- Infrequently accessed or frequently changing content ***should*** be located at a central location (or small number of mirror locations), such as at the LA or RBC.

2.8.2 Location based services

Location based services are services that can make an informed choice of what action to take based on where a device or a user is located in the institution. Whilst some location based services are fairly mature (such as printing to the nearest printer) others are less so (such as services based on the location of the user using triangulation of wireless access points). These types of services are likely to continue to be developed and mature over the next few years.

Design criteria

- Institutions ***should*** consider implementing location based services.
- Institutions ***may*** enable users to print to their nearest printer.
- Institutions ***may*** provide custom desktops suited to a particular scenario (such as their location or subject area).

2.9 Collaborative learning tools

As relatively young applications, there are no formal open standards associated with collaborative technologies such as Blogging (web logging), RSS feeds (automated news headline and content syndication) and Wikis (interactive editable web pages), however de facto specifications are starting to appear and it is these that are outlined here.

2.9.1 Instant messaging

Instant messaging (IM) is a form of online real time chat using text, voice or video, allowing learners to chat with peers anywhere in the world, in real time. Currently interoperability between the major consumer IM applications is limited as there are numerous real time messaging protocols in use, largely as components of commercial instant messaging services (for example: AIM, ICQ, MSN Messenger and Yahoo! Messenger). A number of IETF internet drafts are currently in production to define common profiles and common services for gateways between real time messaging systems. There are, however, a number of third party end-user desktop-based utilities available that combine the functionality of the commercial instant messaging services and support connectivity between users of the various commercial instant messaging services. There are also enterprise class IM solutions that allow for managed, secured and monitored environments.

It is important to note that NAT or firewall devices may cause problems when using advanced messaging features and each IM application has its own configuration solution involving the opening of specific TCP and/or UDP ports. Great care must be taken when opening ports so that institution networks are not left unprotected.

[32] http://www.becta.org.uk/nen

Design criteria

- If implemented, IM solutions ***shall*** allow for real time text exchange and presence services.
- If implemented, IM ***should*** be managed, secured, and monitored.

2.9.2 Blogging

A blog is essentially a web application which contains periodic posts on a common webpage. Blogging combines a personal web page with tools to allow comments to be left and to make linking to other pages and blogs and 'trackbacks' – a system that allows a blogger to see who has seen the original post and has written another entry concerning it.

Design criteria

- Blogs ***should*** allow for hyperlinking, trackbacks and comments.
- Blogs ***should*** have the ability to be managed and secured, allowing only authorised bloggers to post messages.

2.9.3 Wikis

Wikis allows users to freely create and edit web page content using any web browser. Wikis typically consist of a space containing pages that can be freely written or edited.

Design criteria

- Institutions ***should*** consider their design and choice of wikis to allow granular access control over the editing of pages.

2.9.4 RSS

RSS (Rich Site Summary or Really Simple Syndication), also referred to as RDF (Resource Description Framework) Site Summary, is an XML application that allows the owner of a website, blog or content repository to announce new items they have published. There are a number of versions of RSS available, but the standard that has been adopted by e-GIF is RSS 1.0, an XML format conforming to the W3C's RDF specification.

Design criteria

- Where institutions make 'news' available on their web site they ***should*** also make an RSS feed available.
- Institutions ***should*** ensure their RSS feeds conform to RSS 1.0 specification[33].

2.10 Minimising administration

Ensuring administrative data is well managed, accessible and stored in an open format means that information is shared effectively, timely and efficiently, both internally and with authorised partners, such as LA/RBCs.

2.10.1 MIS systems

Management Information Systems cover a range of functionality, with the main systems covering an institution's administrative and management information needs, including comprehensive reporting and data exchange tools to meet the needs of internal users (staff and administrators), external stakeholders (including parents, examination boards, LAs, DfES, regional government and the devolved administrations). Recognising the functional complexity of the individual business processes to be supported, the range of such processes and the variety of internal and external stakeholders and systems to be accommodated, institution MIS systems present a complex software development challenge.

Becta is currently investigating ways of maximising the benefits that MIS systems can bring, by establishing a supplier-independent and open interoperability architecture to create the opportunity for

[33] http://purl.org/rss/1.0/spec

improved interoperability at the institution level and at the LA or RBC level. More information can be found in the Becta report: School Management Information Systems and Value for Money [34]

Design criteria

- Institutions ***shall*** install Common Basic Data Set (CBDS) compliant MIS software[35].
- Institution MIS systems ***should*** be client platform independent.
- Institution MIS systems ***should*** link in to their learning platform[36].
- Institution MIS systems ***should*** include the functionality to address the following:
    - Pupil Records
    - Staff/Personnel Management
    - Curriculum Planning
    - Timetabling and Options Planning
    - Staff Cover
    - Pupil Attendance and Behaviour
    - Assessment and Performance
    - Examination Management
    - Special Educational Needs
    - Financial Management
    - Property and Equipment Management
    - Payroll and BACS
- Each of the above business processes ***should*** be able to share data seamlessly between each other irrespective of whether each module is from the same supplier or not.

2.10.2 Electronic facilities management

An electronic facilities management system will enable central management of an institution's environment, security and monitoring of personnel and transactions.

Design criteria

- Institutions ***should*** implement an electronic facilities management system.
- Where institutions implement a smartcard system, smartcards ***shall*** conform to the e-GIF specifications as described at http://www.govtalk.gov.uk/egif/eaccess.asp#table11a.

2.11 E-portfolios

Following the publication of Harnessing Technology: Transforming Learning and Children's Services, all institutions must offer a personal online learning space to store coursework, course resources, results, and achievements. These facilities will become an electronic portfolio, making it simpler for learners to build their record of achievement throughout their lifelong learning. E-portfolio solutions are currently in the early planning stages and institutions are advised to liaise with their LA/RBC before investing in any solutions.

The DfES, Becta and JISC envisage an e-portfolio process supporting elements of learning, recording learning and the assessment of learning through different components and services. Procurement of e-portfolio solutions must reflect the need for these individual components to interoperate fully. Procurement advice must also recognise that many of the functions required by an e-portfolio process are already supported in institutions, through MIS systems and learning platforms. Further information on Becta's work on e-portfolios can be found at http://www.becta.org.uk/partners/.

Design criteria

- Institutions ***shall*** provide learners with access to electronic portfolios[37].
- Institutions ***shall*** only implement components of e-portfolios that are proven to interoperate with one another.
- Institutions ***shall*** consult their LA/RBC before investing in e-portfolio solutions.

[34] http://www.becta.org.uk/corporate/publications/publications_detail.cfm?currentbrand=all&pubid=279
[35] More information about CBDS can be found at www.becta.org.uk/mis.
[36] See 2.6 Learning platforms
[37] Becta and JISC are working together to develop a specification for e-portfolios. Developments will be posted at http://www.becta.org.uk when available.

3 Implementation of ICT security in institutions

Introduction

ICT security is an important issue that must be proactively tackled with vigilance by both the LAs and Institutions. Institutions need to protect their ICT equipment, curriculum and administration data and also consider the health and safety of all network users.

ICT security is the set of procedures implemented to prevent the unauthorised access, abuse, alteration, or denial of access to knowledge, data or resources. Security is achieved by implementing a suitable set of controls, which comprise policies, practices, procedures, organisational structures and software functions.

This section of the specification details the following five different areas of ICT security; security policies, physical security, data security, network security and internet and remote access security. Each area addresses the controls that need to be implemented in order to maintain an appropriate level of ICT security. All areas concentrate on best practise and common sense controls and are based on the BS 7799 standard but have been amended for the educational sector[38]. These controls provide the general standards by which institutions can securely operate. Institutions may need additional controls based on their local or regional requirements.

3.1 ICT security policies and procedures

Objective: To provide management direction and support for ICT security

The reasons for adopting a formal policy on the security of information are twofold; to provide a framework for best operational practice, so that the institution is able to minimise risk and respond effectively to any security incidents which may occur; and to ensure that the institution complies with relevant legislation in this area.

3.1.1 ICT security policy

An ICT security policy is a document that succinctly states (but is not necessarily limited to) the institution's essential security procedures and policies. It is important to include the institution's guidelines and procedures for everyday security practice, definition of responsibilities, ICT emergency procedures, appropriate, enforceable sanctions and refers where appropriate to supplementary documents. It needs to be short, easily understood, realistic and be reviewed periodically alongside other strategic documents.

Design criteria

- Institutions ***shall*** produce a short easily understood and realistic ICT security policy.

Appendix B contains a draft security policy, which institutions may use as a guide to creating their own policy.

3.1.2 Security Operating Procedures

Security Operating Procedures (SyOps) are short documents, written for individuals and groups, detailing their responsibilities as users of systems. They explain, in short sentences, what is and isn't permissible on the system. In many commercial environments users must sign as having read and understood SyOps which relate to them. It is for institutions to decide whether this is appropriate for their institution (for example this is unlikely to be suitable in many primary schools), but institutions need to agree the policy with staff and how best to circulate the key messages, for example, through posters, regular verbal reminders to learners, key messages attached to appropriate ICT devices etc.

[38] Whilst BECTA advocates a standards-based approach to ICT security, it is acknowledged that to follow BS7799 and RFC 2196 will be difficult and time consuming for the majority of institutions.

Design criteria

- Institutions ***should*** produce System Operating Procedures.
- Adult users and guests of institutions ***should*** sign to indicate their agreement with the procedure.
- Educators ***should*** encourage learners to adopt the practices.

An example set of SyOps has been attached at Appendix C which institutions may use as a guide to creating their own policy.

3.2 Physical security

Objective: To prevent unauthorised access, damage and interference to premises, assets and information

Physical security, although one of the least technical methods of security, is one of the most important to consider. This document deals with the physical security of the ICT equipment and data of an institution. Advice regarding security of physical entry to an institution's premises must be sought from the appropriate sources at the institution's LA.

3.2.1 General physical security

Most physical security controls are common-sense and centre on the protection of information assets and preventing theft/unauthorised removal.

Design criteria

- Sensitive material ***shall*** not be left unattended or unsecured.
- Sensitive information sent to printers ***shall*** be removed from the printer immediately.
- Workstations ***should*** be password protected when left unattended, unless the area has been physically secured.
- Padlocks/equivalent controls **may** be used to protect workstations and laptop computers. This includes workstations that are built into desks or are physically bolted/secured to furniture and Kensington locks for laptops.

Physical Security	Essentials/Essential Upgrade	Enhanced Upgrade
	• Locate servers in secure areas/cupboards and control access.	• Secure valuable ICT equipment (using padlocks, desk locks etc.)

3.2.2 ICT resource management

It is extremely difficult to protect an institution's ICT resources unless those ICT resources are documented and strictly controlled, thus procedures need to be developed to record all devices and software in a detailed ICT resource register. Access to the register needs to be limited to those persons responsible for the institution's ICT resources with overall audit responsibility lying with a designated individual.

Design criteria

- Procedures ***shall*** be developed to record all devices and software in a detailed ICT resource register.
- The register ***shall*** record the location of a device plus key information, for example, serial number, description, change of use, owner, configuration etc.
- The register ***shall*** record software (including relevant license key, version number, etc) installed upon that device.
- The register ***shall*** record software patches and security updates installed on individual devices.
- Regular audits of equipment ***shall*** take place.
- Overall audit responsibility for the register ***should*** lie with a designated individual.

- **Device loans**

Information, software, equipment or items belonging to the Institution must not be taken off-site without formal approval and it is sensible practice to log out when removed from the premises and log back in when returned. Any log form needs ideally to contain relevant information such as make, model, serial number and peripheral devices. There needs to be a process in place to ensure that long term loan items are checked on a regular basis, with the certificate being updated as a result of such checks.

Design criteria

- Users ***should*** only take devices off-site with formal signed approval.
- Users ***should*** be given guidelines on the use and protection of the equipment when away from the institution.
- Devices which are regularly removed from institutions' premises, ***should*** be audited more frequently.

- **Hardware redundancy**

Hardware redundancy is where a given piece of ICT equipment has a replacement available and configured in case of theft or breakdown. It is wise to establish a pattern of hardware redundancy, if possible as this allows seamless operation of the ICT infrastructure, even if there is an unforeseen problem.

Design criteria

- Institutions ***should*** provide hardware redundancy for end user devices that are critical to learners.

Device Management	Essentials/Essential Upgrade	Enhanced Upgrade
No device management	• Implement an ICT resource register. • Record all devices and software in the register. • Implement software version control. • Protect the register and control access to it. • Perform regular auditing of ICT resources and update the register. • Implement FITS[39].	• Implement device management tool. • Provide hardware redundancy.

3.2.3 Critical systems

Consideration needs to be given to the power supply and hardware redundancy of critical equipment, such as severs and networking equipment. Failover is a system of hardware redundancy that requires that there be a replacement for critical hardware that is configured and running in tandem with the "live" system. If the main system fails, then the user is transparently and immediately transferred to the failover hardware, ensuring seamless function of the system. Redundant pairs are similar to failover models of hardware redundancy, but instead of having a second system running in tandem, the second system is kept in a state of readiness, but inactivity. Whilst this requires less of an overhead for the institution to maintain, it introduces a degree of loss to the system, in that the redundant pair might not be exactly in sync with one another.

Design criteria

- Critical equipment ***shall*** be protected by Uninterruptible Power Supplies (UPS), and ***should*** be tested regularly. Critical equipment ***may*** operate in failover or in redundant pairs.
- System configurations ***should*** be backed up and stored in a secure location and be the responsibility of the Network Manager.

[39] http://www.becta.org.uk/fits/

Device security	Essentials/Essential Upgrade	Enhanced Upgrade
	• UPS critical equipment. • Critical equipment ***should*** be stored in a secure location. • System configurations backed up.	• Provide failover / redundancy for firewalls, router, switches and servers.

3.3 Data security

Objective: To preserve the confidentiality, integrity and availability of information

.

3.3.1 Identification & authentication

Identification and authentication is the process used to determine a user's identity, verify that it is correct and establish accountability. The ability to verify the identity of users is critical for ensuring authorised access to system resources and establishing accountability, being able to prove that a user performed a particular action. Identification distinguishes one user from all others. Authentication is the process of verifying the identity of the user. A user is identified and authenticated by establishing what he knows, such as a user id and password.

- **User Ids**

For a user to gain access to the systems at an educational institution, they must first authenticate themselves as a valid user of that system with a system user Id (username) and password. User ids will generally stay the same throughout the user's attendance at an institution, so they need protecting for far longer than passwords. Currently user ids are locally or regionally controlled and thus the use and definition remains the responsibility of the relevant Institution.

Design criteria

- User ids ***should*** be changed when compromise is feared or suspected.
- Shared (as opposed to personal) User ids ***should*** only be used for the youngest of learners.
- Shared ids ***should*** be protected by as strong/complex a password as possible and ***should*** have limited privileges.
- Users ***should*** be as protective of their id as they would their password; if an attacker acquires your id, they then only have to crack your password to gain system access.

- **Passwords**

A password is a means of authenticating a user's identity. It ought to be known only by that user and it is their responsibility to keep it secret at all times.

Passwords are qualified by their strength. Weak passwords are classed as any that have a limited number of characters (normally less than 6) and contain words from the dictionary or names that are easy to guess. Passwords are made stronger/more complex by increasing the number of characters, including alphabet and numeric characters and punctuation marks. Examples of weak passwords may be *peter*, *abcde* or *icepop*, whereas a password such as *Hgmr3n8*! would be classed as strong. Weak passwords are a common security flaw that can increase Institutions' risk of attack from both internal and external sources. By choosing strong passwords and keeping them confidential, it is possible to make it more difficult for an unauthorised person to access information.

It may seem extremely obvious, but it is very important that users do not share their password with anyone or write them down. If users with administrative privileges need to write passwords down, they ought to be placed in a sealed envelope and handed in to the Institutions main office for safekeeping. Many institutions, especially where the youngest learners are educated, will have relatively simple shared user id and passwords. This scenario can lead to a serious weakness, and thus a limited set of permissions need to be associated with shared passwords.

However, it is also recognised that over-complicated passwords will lead to users writing them down. As this is extremely undesirable, the trade-off must be made between having very strong but unmemorable passwords and those that are less strong, but do not induce users to write them down.

Design criteria

- A formal password policy ***shall*** be adopted by the institution.
- Passwords ***should*** **not** be written down.
- Passwords ***should*** **not** be based on personal information that can be easily accessed or guessed.
- Passwords ***should*** be a combination of letters, numbers, and special characters and ***should*** use both lowercase and capital letters.
- Shared passwords ***should*** be avoided but limited access privileges ***should*** be used where shared passwords are deemed essential/appropriate.
- Passwords ***should*** be changed frequently.

It is the responsibility of the institution to ensure that the password policy is correctly implemented and maintained.

Id & A Security	Essentials/Essential Upgrade	Enhanced Upgrade
	• Define user id policy. • Define the password policy and implement. • Educate all users. • Avoid shared passwords whenever possible.	• Increase password length. • Mandate greater strength, such as upper, lower, numeric and special characters. • Shared credentials must be changed more frequently.

3.3.2 Data backup

There are many reasons why data backup is a crucial requirement for every institution. Users inadvertently delete files or overwrite existing files. Hackers or disgruntled learners/educators may do the same intentionally. Disk drives, fail, and lose all of the data they hold. Additionally, files become corrupted by bad disk sectors, magnetic fields, and improper system shutdown. Disasters, such as flooding or fire, can affect buildings and the systems they contain and, although uncommon, need to be planned for. Beyond the traditional threats, there are new threats to today's systems including viruses and worms.

Institutions depend on their computer systems more than ever. Loss of data is therefore more expensive than ever in terms of lost educational and administrative work and downtime.

Synchronisation is a good way to ensure that users' data is kept up-to-date and backed up when a user is working on a portable device (laptop, tablet, etc). Synchronisation involves a system of two files, one held on the central data repository and the other held locally on the user's portable device. Changes to one file are replicated to the other file whilst the machine is connected to the network, thus keeping both versions as closely synchronised as possible. Therefore, if the data is lost then the backup will restore a copy of the data that is close to identical to the original file (missing only any amendments made after the last synchronisation). Most synchronisation regimes will include version control to ensure that both locations store the newest possible copy of the data.

Design criteria

- Institutions ***shall*** have a backup strategy that includes details of what is backed up, the frequency of backup, storage of back up media (on and off site), recovery procedures, the person responsible for backing up data.
- The person responsible for back up ***shall*** be appropriately trained.
- Institutions ***should*** educate individual users on how to backup their own personal data that is not backed up centrally by the system.

- Users ***should*** only save work to local devices when that device is regularly synchronised or backed up via removable media.
- System backup operations ***should*** be performed on a daily basis and ***should*** be transparent to users.
- Tests ***should*** be performed at regular intervals to verify that data can be recovered from the system backup media.
- Institutions ***should*** perform daily backups of new or changed data complemented by a full weekly backup of:
    - All institution administrative data.
    - All users personal data stored in the network user folders.
    - All data stored in shared areas.
    - All changeable educational data stored on the network.
    - The mail server, or as a minimum, individual mailboxes.
    - Operating system/system state data.
    - All activity and audit log files.
- Media containing daily backups ***should*** be stored in fire proof safes wherever possible and full backups ***should*** be removed off-site to a secure location for safe-keeping.

Data Backup	Essentials/Essential Upgrade	Enhanced Upgrade
	• Create backup strategy, frequency, content and safe storage etc. • Educate users on personal backup • Provide backup media. • Store backups off site. • Whenever possible use fireproof storage safes for media.	• Set up reciprocal off-site backup storage arrangements with other Institutions. • Instigate on-line backup through 3rd party or higher authority.

3.3.3 Virus protection

Viruses are a large threat to ICT systems. Institutions must ensure that they protect their data and devices with anti-virus (AV) software

Design criteria

- All devices, including stand-alone devices and portable ICT equipment, ***shall*** be protected by a recognised anti-virus (AV) package.
- The AV package ***shall*** provide an automatic update facility for virus definition files.
- The software ***shall*** be set to scan any new media detected or files received or opened by any route.
- Institutions ***shall*** ensure that AV packages are up to date and all devices have the most up to date virus definitions.
- All documents and removable media ***shall*** be subjected to an anti-virus scan prior to being transferred onto the Institution network.
- Users ***should*** be educated in the safe handling of any media used to transfer data from one system to another, e.g. floppy disks, memory sticks etc.

Anti-Virus	Essentials/Essential Upgrade
	• Implement AV policy. • Install AV on mail, file and application servers. • Install AV on all stand-alone and mobile computers. • Instruct users in the correct use of anti virus products. • Set AV to scan all new media and received files. • Ensure that automatic updates are enabled to maintain AV programs with current definitions.

3.3.4 Spyware Protection

Spyware, programs that are installed (often automatically and surreptitiously), are an issue for many computers or computer networks. These programs can pick up information from an infected machine and transmit it back to the author of the spyware, where it can be used for a large range of potential uses, from targeted advertising to identity theft. Although the instances of spyware causing large amounts of damage are limited, it is at best annoying, and at worst can consume vast system resources, slowing the operation of the machine to a crawl.

There are a number of products that are able to identify and protect against spyware, and generally they fit into three categories.

Real-time protection, which prevents spyware from being installed, *scanning and removal* of spyware, and *hybrid scanners* which do both. Scanning and removal is usually simpler, and so many more programs have become available which do so. The program inspects the contents of the operating system files, and installed programs, and removes files and entries which match a list of known spyware components[40]. Real-time protection from spyware works identically to real-time anti-virus protection: the software scans incoming network data and disk files at download time, and blocks the activity of components known to represent spyware. In some cases, it may also intercept attempts to install start-up items or to modify browser settings.

Design Criteria

- Institutions ***shall*** have access to spyware protection software
- Institutions ***should*** implement hybrid systems for protection from spyware
- Scanning and removal of spyware ***should*** take place at regular intervals on all an institution's machines
- Institution users ***should*** be educated on the dangers and symptoms associated with spyware

3.3.5 Firewall protection

A firewall is a combination of software and/or hardware that provides a protective barrier between a computer or network, 3rd party systems and the internet. It essentially polices the edge of a network and blocks unauthorised access to the institution's network. Hardware firewalls and firewall software work slightly differently, but in general they act on the same principles.

- **Network firewalls**

It is essential that firewalls are properly installed and configured to protect institutions' systems from unauthorised access. To ensure that this is done in such a way as it does not impede an institution's ability to function efficiently; the institutions, LAs and RBCs will all need to work together to ensure that firewalling is carried out, and that if different rules for different institutions are required that those rules are applied through cascaded firewalls rather than applied as a blanket across all institutions. It is recommended that any institution be subject to only one firewall, thus it is advised that if the RBC provides a firewall, and the institution work with them to agree common rules rather than then applying their own rules on their own firewall. It must be noted that multiple firewalls will impede an institution in applying Quality of Service across their network and their partner's network; and can prevent applications such as video conferencing from working.
However, where institutions have already got an adequate firewall in place and wish to retain this, it is acceptable for them to do so, as long as they liaise with their LA/RBC to ensure that the firewalls do not impede the operation of the network and its applications.

Design criteria

- Institutions ***shall*** seek advice on regional firewall policy from their LA or RBC.
- Unnecessary network ports ***shall*** be closed and the default setting ***should*** be 'deny all'
- If an institution has its own firewall they ***shall*** liaise with their LA/RBC regarding firewall policy.

[40] It is worthwhile noting that spyware is more prevalent on certain operating systems. Some operating systems are currently unaffected/little affected.

- Open network ports for normal network functionality ***may*** include; Port 25 – SMTP (mail); Port 80 – HTTP (internet access) and; Port 161 – SNMP (network and firewall monitoring).

- **Personal firewalls**

Personal firewalls are simple, easy-to-configure firewalls that sit on a user's local machine and prevent unauthorised access by machines from across the internet. It is not advised that institutions install local firewalls on their desktop machines, but they may wish to examine these for use on mobile computers that need to access the internet outside of the control of the institution's network. If an institution decides to use these, then they must put in place appropriate guidelines and policies to ensure that they are managed and kept patched.

Design criteria

- Personal firewalls ***may*** be used for devices used to access the internet from outside the control of the institution's network firewall

Firewall	Essentials/Essential Upgrade	Enhanced Upgrade
	• Purchase & install firewall to protect system and portable ICT. • Configure firewall and backup configuration. • Carry out regular firewall log checks. • Check configuration and backup.	• Operate a failover[41] pair at regional level. • Run SNMP live monitoring of firewall (giving automatic alert).

3.3.6 Audit Trail

An audit trail is a log of recorded activity on a system. The logs allows the Network Manager to identify where further education of users may be needed (such as unsuccessful logons and logoffs) and to record and take appropriate action where the security of the network and data is compromised (attempted alteration of access rights and privileges).

Design criteria

- Institutions ***should*** enable the logging of all the following events:
  - All logon attempts whether successful or not.
  - All logoff attempts whether successful or not.
  - Creation, deletion or alteration of access rights.
  - Creation, deletion or alterations of passwords.
  - Creation, deletion or alteration of system log files.

Audit Trail	Essentials/Essential Upgrade	Enhanced Upgrade
	• Configure operating system to audit events in section 3.3.6. • Ensure there is a chain of command / knowledge to escalate problems to.	• Local training for checking. • Software tools for alerting.

3.3.7 Media security

Any item that can hold computer information is classed as media. This includes floppy disks, CDs, printed output, tapes, memory sticks, etc. Media is easily transportable and therefore requires extra controls to ensure it is not damaged, stolen or accessed by unauthorised persons.

[41] Failover pair provides redundancy in case of failure. Firewall 2 is an exact copy of firewall 1 and is switched in automatically in the event of failure

Design criteria

- Users ***should*** receive guidance in the importance of safeguarding media.
- Sensitive or valuable data stored on media ***should*** be removed as soon as possible.
- Media ***should*** be virus scanned on re-introduction to the system.
- Data stored on media ***should*** be synchronised or moved to the institution's repositories as soon as possible.

Media Security	Essentials/Essential Upgrade	Enhanced Upgrade
No media security.	• Provide user guidance on secure use of media. • Provide user guidance on anti-virus tools. • Provide user guidance on media backup.	• Provide encryption software for users.

3.4 Network security

Objective: To protect networks and their applications against attacks, ensuring information availability, confidentiality and integrity

This section deals with securing the media that data passes over. Data can pass over cabling and wires or can be travel wirelessly via radio or microwaves or infrared technologies.

3.4.1 Wired security

Since all network data in a wired network passes over the institution's cables it is vital that access to network data via any device connected to that cabling is by authorised users with the correct privileges and rights. Without the proper security measures in place, even registered users of the network may be able to access information that would otherwise be inaccessible to them. Wired network traffic can be intercepted and decoded with commonly available software tools once one has physical access to the institution's cabling and/or devices. Unfortunately, the vast amount of wire/cabling inherent in even the most basic LANs provides many points for unauthorised access.

- **Cabling security**

One of the simplest ways by which a member of an institution could cause network disruption is by damaging or removing network cabling. Careful placement of cabling (such as behind walls and in wall cavities), and cabinets where cabling terminates, as well as careful management of the cabling is, therefore, essential.

Design criteria

- Unused patch leads ***shall*** be removed from network equipment.
- Routing and switching cabinets ***shall*** be locked and all keys strictly controlled.
- Cables into institutions or between buildings ***should*** be located underground or be adequately protected from physical interference.
- Network cabling ***should*** be protected from unauthorised interception or damage by utilising wall cavities and behind walls wherever possible.
- Regular checks ***should*** be made to ensure that all cables are routed to their correct terminating equipment.
- Unused ports on network equipment ***should*** be disabled or physically taped over.

- **Eavesdropping**

Perhaps the most difficult threat to detect is someone just looking at (and possibly copying) raw data on the LAN. Wired networks are particularly vulnerable to eavesdropping (unauthorised user looking at and possibly copying data from the network). Inexpensive and readily available programs can allow anyone with physical access to the network to read, capture, and display any type of data packet sent over the network. Thus, regular audits need to be carried out to ensure that no such equipment or software is being improperly used.

Design criteria

- Regular audits ***shall*** be carried out to ensure proper use of network equipment and associated software.

Wired Security	Essentials/Essential Upgrade	Enhanced Upgrade
	• Remove all unused cables from network equipment. • Lock all switching cabinets. • Network equipment ***should*** be located in secure areas/cabinets. • Carry out regular checks of all network and end equipment cabling.	• Use different colour cables for different systems. • Utilise wall cavities and behind walls for network cabling. • Unused network ports to be disabled.

3.4.2 Wireless

There are a number of basic security settings that are provided by an access point (AP) or the management software of the AP. The basic premise of network security is to only let authorised users and devices onto the institution's network. Unfortunately, WLAN broadcast their signals over substantial distances (often in excess of 100m) and these signals cannot be contained by physical barriers in the same way as an Ethernet network. Thus, in the case of WLANs, institution networks and the data they carry are open to a number of different attacks including

- Attack via rogue APs[42].
- Attack via interception of wireless signal.
- Attack by attempted unauthorised network access from outside of the institution's buildings.

- **Basic WLAN security**

Much WLAN security simply requires some basic security controls to be put in place by the institution. Virtually all current APs come supplied with management software which, if used properly, can offer a basic level of security. Many of these security controls will deter the majority of unauthorised users from trying to gain access to the institution's network and services.

Default settings and Access control lists

All APs come with default settings. The default settings from some manufacturers are common across all APs in the manufacturer's range. This means that the network name that is broadcast by the AP can tell an authorised network user information about how to break into the institution's network. To enable personalisation and security functions to be managed, an AP usually is supplied with management software that often has a combination of the following features: Turning off the broadcast of SSID (network name); changing the name of the SSID; MAC address recognition; limiting IP range where the AP acts as a DHCP server; setting maximum number of clients that can associate with an AP; ability to manage AP over the WLAN; and setting the channel to be used for the WLAN.

Intrusion detection

Intrusion detection whether carried out manually using a simple piece of wireless detection software or using a fully featured Intrusion Detection System (IDS) is an important part of WLAN security. If an institution knows what APs and networks are authorised they will be able to quickly identify those networks that are unauthorised. Unauthorised networks could be located by a range of means including an SSID that was invalid or an AP using a wireless channel that was not authorised by the

[42] An AP attached to a WLAN that has no authority to be there placed by an uninformed but authorised user or by someone (which could include an authorised user) for illegal/malicious reasons.

institution. Intruders to a network may also be identified by such things as recognising the reuse of MAC addresses.

Firewalls and network segments
A technique used to secure WLANs is one where the WLAN is placed in its own segment of the network and security is enhanced by use of a firewall to separate the WLAN from the wired network (see section 1.4.5 Virtual Local Area Networks. This practice has been usefully deployed in a number of institutions and whilst the use of advanced encryption techniques (see below) mean that this practice could now be seen as less of a priority, it has been deployed successfully in a number of institutions especially where WEP (see below) is the highest form of encryption available.

Design criteria

- Institutions ***shall*** change default settings of WLAN equipment.
- Institutions ***should*** give their WLAN networks a name (SSID) that cannot be associated with the institution.
- Institutions ***should*** disable SSID broadcasting.
- Institutions ***should*** employ regular intrusion detection checks.
- IP addresses for WLAN clients ***should*** be limited to the maximum number of devices that could realistically associate with that AP where DHCP and NAT is performed by the AP.
- Institution's ***should*** disable features that allow an AP to be administered via the WLAN.

- **Authentication and encryption**

The encryption standard available with most WLAN equipment until recently was WEP (Wired Equivalent Protocol). This protocol has proven to be flawed and both the IEEE and the Wi-Fi Alliance have worked on improved standards and specifications for wireless encryption. 802.11i is an IEEE standard that was designed to address all the flaws in WEP. As this standard took a long time to be ratified, the Wi-Fi Alliance produced its own security specification entitled WPA (Wireless Protected Access) which had many of the features of 802.11i. The subsequent Wi-Fi Alliance specification entitled WPA2 is a full implementation of the 802.11i standard. Both WPA and WPA2 are seen by the wireless industry as secure; the main difference being that WPA2/802.11i uses an encryption protocol (AES – Advanced Encryption Standard) that offers further enhanced security than the one used in WPA (TKIP – Temporal Key Integrity Protocol). WPA and WPA2 can be implemented by an institution in two different modes.

Enterprise mode offers the most security available to wireless devices. In Enterprise mode an AP blocks access to the institution's network until a user is authenticated (normally via a RADIUS server) and initial keys to be used in encryption are exchanged.

In Personal/ SOHO (Small Office/Home Office) mode the initial key used in the encryption process is configured manually in each device so authentication via RADIUS is not used. The same encryption techniques are used as in Enterprise mode (per user, per packet, per session encryption), but the obvious weak link is that if an initial key is ever shared, then the institution's network could be compromised.

Both WPA and WPA2 can be used in a 'mixed mode' which allows a WPA device to be backwards compatible with another device using a previous wireless security protocol. Unfortunately, in the case of WPA this means that if a WPA device interacts with one using WEP, this greatly reduces the security.

Design criteria

- Institution's ***shall*** use as high a standard of authentication for WLANs as they do for their wired networks.
- Institution's ***shall*** use WPA encryption and ***should*** use WPA2/802.11i security where possible.
- Institution's ***should*** **not** use mixed mode in WPA.
- Institutions waiting to upgrade to WLAN equipment using WPA/WPA2 ***should*** authenticate individual devices via MAC address recognition or ***should*** consider using a separate network segment policed by a dedicated firewall.

- Institutions waiting to upgrade to WLAN equipment using WPA/WPA2 ***should*** limit access to sensitive data over the WLAN.

Wireless Security	Essentials/Essential Upgrade	Enhanced Upgrade
	• Change default settings of WLAN equipment • Use as high a standard of authentication for WLANs as for wired networks • Use WPA encryption	• Disable SSID broadcasting • Deploy regular intrusion detection checks • Use WPA2 encryption with RADIUS

3.5 Internet and remote access security

Objective: To provide a safe environment in which to access information and communicate through the internet

3.5.1 Remote access

Remote access is the ability to get access to a computer or a network from a remote location. Learners, educators and other users working from home, travelling or at another institution may need access to their institution's network. Home users typically get access to the internet through remote access to an Internet Service Provider (ISP). Using dial-up or broadband connections from a desktop, notebook, or handheld computer modem over regular telephone lines are common methods of remote access. Remote access is also possible using a dedicated line between a computer and the institution local area network.

A remote access server is the computer and associated software that is set up to handle users seeking access to the network remotely. Sometimes called a communication server, a remote access server usually includes or is associated with a firewall, to ensure security, and a router that can forward the remote access request to another part of the Institution network. A remote access server may include, or work with, a modem pool manager so that a small group of modems can be shared among a large number of intermittently connecting remote access users. A remote access server may also be used as part of a virtual private network (VPN).

There are several varieties of remote access security protocols including IPsec, PPTP (Point-to-Point Tunnelling Protocol), L2TP (Layer 2 Tunnelling Protocol), SSL and S-HTTP.

- **IPsec**

Internet Protocol Security, IPsec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes:

- Transport – Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched; and,
- Tunnel – The more secure Tunnel mode encrypts both the header and the payload.

On the receiving side, an IPSec-compliant device decrypts each packet.

For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

- **PPTP**

Point-to-Point Tunnelling Protocol is a technology for creating VPNs. Because the internet is essentially an open network, the Point-to-Point Tunnelling Protocol (PPTP) is used to ensure that messages transmitted from one VPN node to another are secure. A PPTP client is included in some operating systems, and the protocol makes few demands on network bandwidth. These two facts make PPTP an affordable option for those who don't have specific (hardware-generated) requirements for other VPN protocols.

- **L2TP**

An L2TP client is standard in some operating systems. It can build tunnels across networks other than IP, so frame relay or ATM links can be included in a standard security plan. L2TP's flexibility makes it an affordable option for institutions with multiple network and link technologies in use, since the ICT staff must learn to deploy and support only a single VPN protocol.

- **SSL**

Secure Sockets Layer is a protocol developed for transmitting private documents via the internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection. All modern web browsers support SSL and many web sites use the protocol to obtain confidential user information securely. By convention, URLs that require an SSL connection start with *https* instead of *http*. Using SSL for WebMail, POP, IMAP and SMTP ensures that all of your communications between your personal computer and your email service provider's computers will be encrypted. Your message content, username and password will be hidden from eavesdroppers; but only while in transit between you and your service provider! Using these SSL services does not protect your messages once they leave your ISP SMTP Server and head to their destinations. While it doesn't protect your message content it does completely protect your username and password from detection, and this is very important as it helps mitigate identity theft, the sending of false messages, etc.

- **S-HTTP**

Another protocol for transmitting data securely over the World Wide Web (WWW) is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary, rather than competing, technologies. Both protocols have been approved by the Internet Engineering Task Force (IETF) as a standard.

There are numerous methods of securing communications and traffic between the institution and the remote user. This paper does not wish to mandate the solution that each institution must use, as all solutions will be dependant on, not only the operating systems and the network devices being used, but also affordability. Institutions must investigate the functionality already provided by their equipment, operating systems and browsers and develop their remote access requirements from there.

The Remote Access scene is constantly changing and this is an area in which it is anticipated that there will be many advances in the near future. Currently, the lack of open standards based VPN solutions at prices that are cost effective for institutions to implement means that it is advised that institutions look to providing remote access via a standards based browser interface. More advice and analysis of this can be found in section 1.6.1 Remote Access.

Remote Access	Essentials/Essential Upgrade	Enhanced Upgrade
	• Implement web-based remote access.	• Implement hardware VPN solution.

3.5.2 Email security

The three principles of ICT security involve maintaining the confidentiality, integrity and availability of information resources. These three principles can also be directly applied to the area of email security. A weakness in any one of these three key principles will undermine the security of an email system and open the door to exploitation.

Virus writers are continuously looking to exploit vulnerabilities in systems and software and make every attempt possible to cover their tracks. Spammers are constantly changing the appearance of spam and masking its source to avoid it being blocked before it reaches its target.

- **What can be done?**

There is a variety of mail security products on the market today, aimed at addressing the various threats to email security. They come in the form of special software that you can load on an existing mail server, or on a dedicated mail gateway platform, or in the form of a hardware appliance that acts

as an email gateway (the more expensive option). Another option for institutions is to outsource mail security to a service provider.

Some of the common features in mail security products today include content filtering services, such as anti-virus, anti spam, script removal, blocking of attachments by file type, and scanning of inappropriate content.

Institutions must install a reliable virus scanner, which screens all incoming and outbound messages and attachments for email viruses and worms. It is not enough for a package to just detect a virus – a good security tool must be able to block the infected documents or clean them before the email reaches the addressee. Additionally, the anti-virus solution must notify the recipient and/or Network Manager of the email-borne virus. This way, viruses are stopped in their tracks before they do any harm, and senders can be alerted that their systems are infected.

The scanner must perform its detection tasks within a reasonable time. The scanner must be able to create a report file in a specified directory (at least not on that drive where viruses are located) and the full path of scanned files must be present in the report file. Long paths MUST NOT be abbreviated, e.g. by using "..." instead of several intermediate directory names. Shortening file paths is acceptable when displaying them on the screen, but not in the report file. In addition, the scanner must be able to run unattended – and it must not stop on each infected object and request user input. When scanning has completed, the scanner must be able to exit automatically and not wait for additional user intervention.

An efficient anti-spam tool ought to be installed, which will pick up words and phrases that usually appear in unsolicited commercial emails and block the unwanted message from entering the system. While preventing inconvenience to recipients, this saves the institution time that users would otherwise have wasted reading and deleting junk mail. Advanced anti-spam features include the detection of incorrect 'From' headers and addresses in the email body, typical spam practices, as well as the facility to be programmed to block emails containing any phrases the institution chooses. Another essential ingredient is the ability to prevent spammers from using the institution's system to send out vast quantities of mail, a practice known as mail relaying.

Also worth considering and effective against spam is a quarantining feature that deters email messages with dubious content from going through. This feature acts as a kind of clearinghouse, allowing an authorised person to approve the filtered messages before they are sent or received.

A content checking tool is a must to prevent users from sending out sensitive information via email. This tool automatically scans the contents of each message being mailed. To be effectual, this tool ought to link to a quarantining feature that isolates emails with suspect content and prevents them from being sent unless an authorised person within the institution has approved the message.

Design criteria

- Institutions ***shall*** install a reliable virus scanner, which screens all incoming and outbound messages and attachments for email viruses and worms.
- A content checking tool ***shall*** be installed.
- An efficient anti-spam tool ***should*** be installed.
- A quarantining area ***should*** be implemented for dubious incoming and outgoing emails.

Email	Essentials/Essential Upgrade	Enhanced Upgrade
	• Install AV product. • Implement anti-spam product. • Install content checking tool.	• Install hardware appliance that offers all essential upgrade features.

4 Network Technologies in institutions

Introduction

Institutional infrastructure must be approached holistically; the essential nature of a connected ICT strategy is such that no one component can be taken in isolation from the others. It is important to pay attention to individual components to ensure that all functions can be enabled by the technologies deployed. This section addresses the functions of those technologies.

Whilst specifications have been included for technologies to enable common technical functions, it is outside the remit of this section to define specific proprietary technologies for network devices. In addition, it is anticipated that a rigid approach to specifying equipment by arbitrary values (clock speeds and the like) is neither useful nor adherent to EU regulation. Therefore this section defines standards and functionality, rather than values and components.

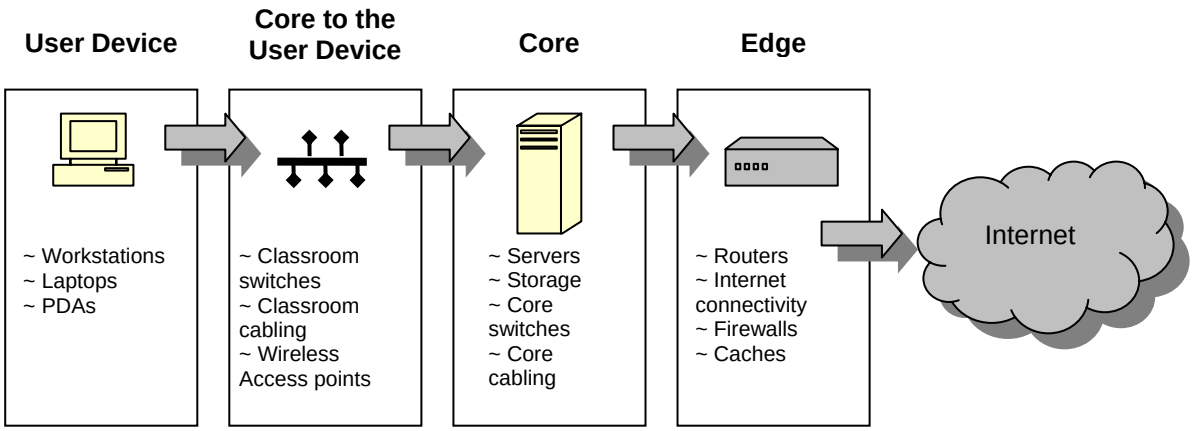

Figure 2 Network technologies addressed in this section

4.1 Network Edge

The Network *edge* is where the Institutional Network (often referred to as the 'LAN') meets the Wide Area Network (WAN). So, for an institution, the network *edge* is likely to be where its network meets the LA network, or for an LA where its network meets that of the RBC. The *edge* is an institution's link to the outside world and as such it is vital for communication with other institutions as well as for access to the Internet and the National Education Network (NEN).

The Network *edge* will typically consist of an edge router (or appropriately configured switch) to direct network traffic to the appropriate external devices and to route traffic received to its appropriate recipients. There will also be Firewall protection preventing unauthorised access, though the firewall ***should*** be located at and managed by the LA/RBC (see also 3.3.5). URL filtering ***shall*** be implemented to prevent access to inappropriate web content (implemented regionally and cascaded as with the Firewalls)(see also 2.3 and 2.7.3), and a caching system will help to make best use of the institution's connectivity by caching educational content(see also 2.8.1). All this equipment will have a high bandwidth connection to the network core.

4.1.1 Defining functions of the Edge

The Network *edge* is vital for communication with the outside world, and so;

- ***shall*** be connected directly to the network core.
- ***shall*** contain a means of communicating and routing network traffic to the correct locations.
- ***shall*** be adequately protected against any unauthorised attempts to access the institution's LAN from outside.
- ***shall*** have the ability to accept incoming traffic from authorised sources.
- ***should*** be equipped with a means of caching data, so that potential bottlenecks in educational traffic can be mitigated.

- ***should*** be able to filter web traffic based on URL (where it cannot, URL-based web filtering ***shall*** be implemented at the LA/RBC).

4.1.2 Enabling the Edge

Universal functions for Edge equipment

- *Edge* equipment ***shall*** have secure management capability allowing alterations to be made to configurations of this equipment by authorised and authenticated administrators.
- Configuration profiles of the *Edge* equipment ***shall*** be able to be backed up.
- Security ***shall*** be addressed whether this is by the router or by a separate hardware or software firewall at institutional or regional level.
- All *edge* equipment ***should*** be protected by UPS equipment (see Core section for specifications for UPS equipment)
- Secure management capability ***should*** be available remotely as well as locally.
- There ***should*** be a gigabit connection between *edge* equipment and the LAN core

Redundancy

- Redundancy ***should*** be provided for the key network *edge* equipment, whether that redundancy is provided by the institution having spare equipment or by a service agreement with a replacement clause. The primary concern is the router, allowing replacement of the unit in case of failure.
- Firewall configuration ***should*** always be backed up to allow fast reapplication of the policies if problems occur.
- Access to a backup firewall ***may*** be provided
- ISDN or ADSL backup ***may*** be provided and configured in case of router failure.

Accessibility

There are no anticipated accessibility issues with the network *edge*.

4.1.3 Technologies for the Edge

Routing Devices

Routing will almost always be carried out by an *edge* router, but in some situations this function can be carried out by a Layer 3 network switch with LAN extension services. The following requirements apply equally to any routing solution.

- Routing devices ***shall*** support open standard routing protocols such as OSPF or IS-IS.
- Routing devices ***shall*** support standards based encapsulation (eg: PPP or PPPoE)
- Routing devices ***shall*** support DNS and be DHCP and NAT capable[43](see also 1.1.5).
- Routing devices ***shall*** support a minimum of 8Mbps/2Mbps for egress traffic (as per the DfES guidelines[44]).
- Routing devices ***shall*** have upgradeable software based feature sets.
- Routing devices ***shall*** support multicast protocols.
- Routing devices ***shall*** support access control lists.
- Routing devices ***shall*** support the following QoS/Traffic management standards:
    - Differentiated Services (DiffServ) and MPLS (Multiprotocol label switching) for the QoS Service Model [45]
    - Low Latency Queuing (LLQ) for Congestion Management
    - Differentiated Services Code Point (DSCP) for Classification/Marking

[43] DNs and NAT are best handled at LA/RBC level and their results cascaded down to the institution
[44] http://www.teachernet.gov.uk/docbank/index.cfm?id=8056
[45] http://www.ja.net/development/qos/call-for-expression-of-interest-0506.pdf Diffserv is the model proposed by UKERNA for the QoS trial.

  - Diffserv-compliant Weighted Random Early Detection (WRED) for Congestion Avoidance
  - Traffic Control. Use Traffic Shaping and Policing i.e. Committed Access Rate (CAR)
- Routing devices ***should*** be scalable and modular to allow the addition of extra modules to increase the number of ports, provide additional modes of connectivity (such as adding fibre ports to a predominately ethernet provisioned router) and increase the amount of onboard memory, or similar.
- Routing devices ***should*** suffer minimal performance degradation when using QoS or data compression.

Firewalls

It is vital to consult with LA/RBC contacts with regard to implementation of firewalls, so that duplication of effort is minimised and disruption to services such as video-conferencing is eliminated. It is best if firewalls are cascaded to the institution from the LA/RBC.

- Firewalls ***shall*** comply with the specifications given in section 3.3.5
- Firewalls ***shall*** also comply with the NEN design document security requirements[46]

URL filters

- URL filters shall comply with section 2.3

Caching and Content Delivery

It is vital that institutions consult with their LA/RBC partners when implementing caching and content delivery systems in order to ensure that such systems are compatible with one another.

- Caching and Content delivery systems ***shall*** comply with section 2.8.1.
- Caches ***shall*** not be located in-line with the institution's broadband connection.

4.2 Network Core

The network *core* is fundamental to the operation of the institution's network. Whilst the network *core* is generally located within each institution, some of the functions of the *core* are often enabled outside of the institution itself e.g. at the LA or by a single institution within a cluster of institutions. Key hardware and software that enables the network resides within the *core*. The LAN backbone, primary servers and network management all fall within the remit of the *core*, controlling and routing the flow of network traffic throughout the institution.

A typical network *core* will consist of a number of network switches, cascaded intelligently, into which the cabling backbone of the network feeds. This cabling will be capable of high data rates (defined in section 1.1.3). Resident in the *core* will be one or more servers providing a wide range of services, from application services through to web hosting and e-mail functions, as required by the institution. Storage sufficient to the institution's needs will be provided at the *core* and all equipment will be protected by power management devices.

4.2.1 Defining functions of the Core

- The *core* ***shall*** enable the highest data rates within the institution, and ***shall*** ensure the integrity of network packets falls within locally defined tolerances.
- The *core* ***shall*** provide management opportunities and monitoring tools to ensure that high network performance,
- The core ***shall*** provide server functions for the institution, including, but not limited to, data storage, application services, and security management
- The *core* ***shall*** support CoS throughout.

[46] http://getconnected.ngfl.gov.uk/docs/security.doc

4.2.2 Enabling the Core

Universal functions for *Core* equipment

- Manageable *core* equipment ***shall*** have the capacity to be managed both directly and remotely
- Management services ***shall*** have access to them secured by a unique ID and password (see also 3.3.1).
- *Core* equipment ***shall*** support 802.1Q to enable priority queuing and VLAN functionality (see also 1.4.5).
- *Core* equipment ***shall*** support 802.1p priority queues for CoS support
- *Core* equipment ***shall*** be cascaded in a manner that ensures the speed and integrity of network packets is not adversely affected
- All *core* equipment ***should*** be protected by power management hardware

Redundancy

Redundancy in the *core* is exceedingly important. If the *core* fails then the entire network will fail. Whilst it is recognised that it is not usually possible to hold a number of hardware devices in reserve in case of failure;

- Institutions ***shall*** have contingencies in place to enable the timely replacement of key *core* equipment.
- Backups ***shall*** be taken of the users files so that they can be restored in case of failure. The processes for this are covered in section 3.3.2[47].
- Institutions ***should*** implement network fault finding software, and ***should*** monitor the network[48]

Accessibility

There are no anticipated accessibility issues with the *Core*.

4.2.3 Technologies for the Core

Switches

Whilst the same is true of most hardware, the differences in available features, quality and network performance between budget switches and higher priced switches are far more noticeable. As an institution's *core* switches are fundamental to the reliable operation of the network, it is vital that an institution ensures that its *core* switches are of high quality. Budget switches can require more support, are often more prone to failure and can cause network packet loss at unacceptable levels; this can prove more expensive in terms of total cost of ownership over the lifetime of the switch.

Thus *Core* switches:

- ***shall*** be capable of full duplex and auto-sensing.
- ***shall*** employ store and forward, fragment free or adaptive switching
- ***shall*** have the capacity to be managed both directly and remotely
- ***shall*** support 802.1Q to enable priority queuing and VLAN functionality.
- ***shall*** support 802.1p priority queues for CoS support
- ***should*** have latency of no greater than 20 Microseconds for a 64-byte frame.
- ***should*** employ SMON as defined by RFC 2613[49]
- ***should*** support Power over Ethernet as defined by 802.3af
- ***should*** be scalable and modular to allow expansion through the addition of extra modules.
- ***should*** be over-provisioned with ports to allow for future expansion of the network OR have the capability to provide this at a later date.

[47] This will also be expanded upon in FITS OM, expected in Q1 2006
[48] This process will be covered in further detail in FITS OM, which has an anticipated release date of Q1 2006.
[49] http://www.rfc-archive.org/getrfc.php?rfc=2613

Cabling

Cabling requirements can be found in section 1.1.3; and are to be referred to when specifying cabling installations and upgrades.

Servers

Servers are key to the efficient working of an institution's ICT, the applications that they run and the functions they perform are vital. Therefore, it is important for an institution to have a clear vision of what software they require a server to run and what functions it must perform before entering into the procurement process. Applications will give a minimum and a recommended specification required to run them, and it is important that the servers procured meet the recommended specifications for **all** software that they are required to run.

- Servers ***shall*** use dedicated server operating systems
- Servers ***shall*** be equipped to enable data backup locally or remotely[50] (see also 3.3.2)
- Servers ***shall*** have processing power, RAM and storage sufficient to cope with all applications that an institution requires them to run.
- Servers ***should*** be connected to *core* switches with at least gigabit-rated NICs that support full-duplex operation.
- Servers ***should*** have disk redundancy features via RAID or similar

Server Operating Systems:

- ***shall*** provide a kernel, disk operations, and file management
- ***shall*** be network enabled
- ***shall*** provide user administration functions
- ***shall*** have administration functions protected by authentication techniques.
- ***shall*** be currently supported by the manufacturer or Distro.
- ***should*** provide logging of errors and access (see also 3.3.6)

Storage

Storage is vital for users in an institution. Storage can be provided on dedicated file servers, on a Storage Area Network (SAN) or on a multi-purpose server (if the institution has a small number of users).

- Where SANs are used, they ***shall*** use the iSCSI standard as defined in RFC 3720[51] or FCIP if a fibre channel solution is used
- Where SANs are used, they ***should*** be managed in accordance with ANSI INCITS 388-2004[52]

Power management

- UPS systems ***shall*** carry the CE mark for electrical equipment[53].
- All UPS systems ***shall*** comply with UL1449[54]
- All UPS systems ***shall*** also comply with the relevant IEEE standards from the 62 series[55]
- UPS ***shall*** provide enough power to protect all mission critical *core* equipment for at least 10 seconds hold-up time.
- UPS systems ***should*** support SNMPv3 for management functions.

[50] It is acknowledged that not all servers will require all data/configuration backed up, however it is anticipated that every server will have some appropriate configuration or data requiring back up procedures
[51] http://www.faqs.org/rfcs/rfc3720.html
[52] http://www.ansi.org
[53] http://www.dti.gov.uk/strd/cemark.html
[54] http://ulstandardsinfonet.ul.com/scopes/1449.html
[55] http://www.ieee.org/portal/site

Management Tools

- Network management tools ***should*** support SMON.
- Network device management tools ***should*** use SNMPv3
- Network monitoring ***should*** use RMON for monitoring and management

4.3 Network Core to the User Device

The Network *core* to the user device is the hardware that runs from the network backbone to the *user device*, providing access to server functions from the user device. Typically this will be cabling run from the server room, to LAN switches and WLAN access points in the classroom.

4.3.1 Defining functions of the Core to the user device

The *core* to the *user device*

- ***shall*** provide a minimum of a 100Mbps rated connection to user devices when wired technologies are applied (see section 1.1.4)
- ***shall*** provide adequate network connections for all user devices in any given location, with the capacity for extra ports for future expansion.

4.3.2 Enabling the Core to the user device

Universal functions of *Core* to the user device equipment

- All cabled networking equipment ***shall*** be rated to at least 100Mbps. (see section 1.1.4)
- All equipment ***should*** be able to support 802.1Q. (see section 1.5)
- Any wireless LAN access points ***should*** be rated to provide signalling rates in excess of 50Mbps (although it is acknowledged that actual data rates will be less than this), and ***shall*** conform to the specifications set out in 1.2.

Redundancy

Whilst the impact of a failure in the *core* to *user device* is less than a failure in the *core*, it can still have an adverse effect upon learners and educators in an institution.

- Therefore this segment of the LAN ***should*** be monitored as a part of the ongoing *core* monitoring, and there ***should*** be a process in place to replace or repair faulty equipment in a time scale that will not disrupt an institutions functions unduly.
- Institutions ***should*** ensure that where network ports are located, those locations are over-provisioned with ports, to allow for expansion and replacement ***should*** faults occur. This ***shall*** also apply equally to switch ports.

Accessibility

There are no anticipated accessibility issues with the *core* to the user device.

4.3.3 Technologies for the Core to the User Device

Switches

The switches referred to in this section are those located outside the *core* e.g. in classrooms, staff areas, offices; used to provide traffic aggregation and to expand capacity. As such the specifications are less rigorous than the institution's *core* switches.

Switches:

- ***shall*** be capable of full duplex and auto-sensing.
- ***shall*** employ store and forward, fragment free or adaptive switching
- ***shall*** support 802.1p priority queues for CoS support (see section 1.5)
- ***should*** have the capacity to be managed both directly and remotely
- ***should*** support 802.1Q to enable priority queuing and VLAN functionality. (see section 1.5)
- ***should*** employ SMON as defined by RFC 2613
- ***should*** support Power over Ethernet as defined by 802.3af

- ***should*** be over-provisioned with ports, with the capacity to implement (through expansion of the switch or similar) additional ports or have the capacity to expand to provide this.

Cabling

Cabling requirements can be found in section 1.1.3; reference shall be made to this when specifying cabling installations and upgrades.

Wireless Access Points

Wireless technologies requirements can be found in section 1.2. Institutions ***shall*** make reference to these before procuring Wireless LAN equipment for new installations or upgrades.

4.4 User Device

The user device is the interface to the end user, and as such it shall be equipped with applications to allow the manipulation and viewing of data. The design criteria are intended to be applied to workstations, PDAs, laptops and similar rather than Interactive Whiteboards or Data Projectors, however advice on provisioning IWBs and Data Projectors is offered in section 4.4.3.

4.4.1 Defining Functions of the User device

- The user device ***shall*** provide a user interface (appropriate to the user) for an institution's users, allowing them to access and interact with their files, network resources and content held outside the institution (whether this be directly or through a caching system).
- ***should*** allow manipulation of text, images and video as well as providing an audio interface (see section 2.)

4.4.2 Enabling the User device

Universal functions of User device Equipment

All network connected user device devices

- ***shall*** have the ability to view office productivity documents
- ***shall*** be equipped with a current version of a standards based web browser (see also 2.3).
- ***shall*** have a network interface able to transfer data at rates commensurate with the *Core* to the user device hardware serving the device.
- ***shall*** require authentication from an institution's user before granting access to secured areas of the LAN[56].

Redundancy

- Institutions ***shall*** ensure that user device devices are subject to a maintenance policy that ensures sufficient availability for the needs of the institution's users. This can be through the maintenance of a pool of replacement user device equipment, or service level agreements that ensure that faulty devices are fixed in a timely manner.

Accessibility

- Institutions ***shall*** ensure that access to user device equipment is available to all users irrespective of disability or special needs. Specialist equipment ***shall*** be managed in such a way as to ensure that those users can access that equipment where and when they require it and that appropriate network services are available via that equipment

[56] Authentication is unnecessary in certain circumstances – should an institution wish to provide an internet café style service to its users, authentication may prove a hinderance. However, authentication shall be used when accessing non-publically available information.

4.4.3 Technologies for the User device

Workstations

Workstations are incredibly diverse in their form and function, and requirements are entirely dependent on the purposes for which they are intended and the type of network to which they are attached. The most basic workstations will provide office productivity applications and internet access, however specialised (and most likely more powerful) workstations will be required for applications such as video editing and CAD/CAM. Institutions shall, therefore, examine the minimum and recommended specifications for the software (applications and Operating System) that they wish to run, and install workstations that exceed the recommended specifications. It is, of course, important to consider not only the current configuration of the network, but also look to the network's future and ensure that any workstations meet the specifications for software that they will be required to run throughout their lifespan. (See section 2)

There could appear to be financial savings to be made through the purchase of reconditioned equipment, however such equipment is almost always supplied with no warranty, and is unlikely to have as long a lifespan as new equipment.

- Workstations ***shall*** exceed the recommended specifications for the operating system and applications that they are expected to use.
- Workstations ***shall*** interface with the network at data rates of at least 100Mbps (see section 1.1.4).

Portable Devices[57]

Portable devices follow many of the same guidelines as workstations. It is essential to ensure that they exceed the recommended specifications for the software that they will use, and they are equally subject to the guidance on new equipment as opposed to reconditioned equipment. With few user serviceable parts, it is very important that they have some form of warranty from the manufacturer or service provider.
There are some additional requirements that portable devices shall meet. In particular, battery life needs to be adequate to allow independent working. Also, many laptops and tablet devices will be used with interactive whiteboards/data projectors and often the distances covered are longer than USB can adequately support (USB has a cable limit of 15m); in these cases the device needs to be equipped with a serial port or a converter to allow this connection to be made.

- Portable devices ***shall*** exceed the recommended specifications for the operating system and applications that they are expected to use.
- Battery life ***should*** exceed 1 ½ hours under full CPU load with full screen brightness.
- Laptops and tablet devices ***should*** have the appropriate ports or converters to allow them to connect to other equipment.
- Portable devices ***should*** include wireless networking capability.

Interactive Whiteboards and Data Projectors

These devices should be specified in accordance with the Interactive Whiteboards Project specified at http://www.becta.org.uk/leaders/leaders.cfm?section=5&id=3155

[57] In this case the term "Portable Device" is used to mean laptops, PDAs and Tablet PCs and does not include peripherals such as cameras which may be networked.

Appendix A – How to give feedback on this discussion document

Introduction

It is of paramount importance that the technical specifications set out in this document are shared by those who work in and influence the use of ICT in education. Whilst these specifications will be of particular importance to institution Network Managers and educational ICT suppliers and consultants, there will also be others who wish to provide feedback and offer their own opinions

Comments should be emailed to techstandards@becta.org.uk or mailed to:

Techstandards
Technical policy, standards and delivery team
Becta,
Millburn Hill Road
Coventry
CV4 7JJ

Name (optional)	organisation:	Contact details (optional):

General comments or observations e.g. document content, document format, general omissions,…

Specific comments:		
Document section (e.g. 3.2.1)	**Comment:**	**Possible rewording:**

Appendix B – Example of security policy document

ICT SECURITY POLICY

OBJECTIVE

The objective of ICT security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.

POLICY

The purpose of the Policy is to protect the institution's information assets from all threats, whether internal or external, deliberate or accidental.

It is the Policy of 'Institution' to ensure that:

- Information will be protected against unauthorised access.
- Confidentiality of information will be assured.
- Integrity of information will be maintained.
- Regulatory and legislative requirements will be met.
- Business continuity plans will be produced, maintained and tested.
- ICT security training will be available to all staff.

All breaches of ICT security, actual or suspected, will be reported to, and investigated by the 'ICT security manager'.

Standards and Procedures will be formulated to support the policy, which will include:

- Security Operating Procedures
- Data back-up Procedures
- Asset classification and control.
- Physical and environmental security.
- Systems development and maintenance.
- Staff/pupil compliance
- Acceptable use

The 'ICT security manager' has direct responsibility for maintaining the Policy Standards and Procedures and providing advice and on their implementation.

It is the responsibility of each member of staff to adhere to the Policy, Standards and Procedures.

Signed …… Date ……

Head Teacher/'ICT Security Manager'
'Institution'

Appendix C – Example of User SyOps

Scope

The following Security Operating Procedures (SyOPs) apply to all (*Insert system name*) users, independent of any explicit role they may have on the system. All (*Insert system name*) users have to comply with these SyOPs, in addition to those specific to their roles.

Remember, non-compliance with the SyOps may lead to disciplinary action being taken against you.

General Dos and Don'ts for all 'Insert system name' Staff

As a (*Insert system name*) User, you are to:

- Sign as having read and understood the Security Policy and SyOPs produced for (*Insert system name'*) and the security obligations stated in it. The (*Insert system name*) Head Teacher will ask you to do so before commencement of work on (*Insert system name*);
- Attend and implement any security briefings provided by the Head Teacher for all staff working on (*Insert system name*);
- Consult the Head Teacher regarding any proposed changes to (*Insert system name*). These changes could be changes to software, hardware, design, the technical architecture or any procedural changes;
- Ensure that all changes to (*Insert system name*) are clearly documented and that adequate reports and logs are maintained and that they are accountable to you;
- Comply with the (*Insert system name*) Incident Management Procedures. You are to promptly report any unusual suspected or detected attempts to breach security to the Head Teacher or Network Manager. You can contact the Network Manager by phone: ……., pager: …… or email: …….. The Network Manager is to inform the Head Teacher at the earliest opportunity;
- Report all security incidents involving a breach of personnel, hardware, software, communication, document or physical security immediately to the Network Manager and Head Teacher. Keep written details of these incidents for any investigation to follow;
- Complete a 'Security Incident Report Form' *(Insert where this can be found)* and forward it to the Network Manager as soon as practicable. Examples of security breaches are:
    - unauthorised or unescorted visitors;
    - unauthorised access to the institution;
    - compromise of passwords;
    - unauthorised introduction of software;
    - unauthorised modification or tampering with components;
    - unattended terminals left logged in; and,
    - theft of hardware or software.
- Ensure that evidence is collected by the Network Manager and not tampered with in the event of a security incident. You are to co-operate with the Network Manager during such investigations;
- Comply with the (*Insert system name*) Clear Desk and Clear Screen Policy:
    - Lock away all sensitive and valuable documents (paper and magnetic) in cabinets or desk drawers (as appropriate) when the desk is unattended for an extended period - for example when away for meetings, at lunch times, or overnight;
    - Log off computers and laptops (unless a password protected screen saver is in operation on the workstation) when unattended. When you have finished a session on the workstation invoke the password-protected screensaver and at cease of work close down all the applications and log off/shutdown the workstation/laptop and lock the laptop away or secure it through the use of a cable lock;
    - If, in an emergency, you need to leave the office quickly, e.g. a fire alarm, invoke the password-protected screensaver, ONLY IF IT IS SAFE TO DO SO, so that unauthorised personnel cannot use it; and,
- Obtain authorised permission from the Head Teacher/Network Manager when removing any equipment from Institution premises. Each piece of equipment is to be signed out and

returned on time. The Network Manager will check this at set intervals to confirm that they have been returned on time;
- Follow the procedures developed by the (*Insert system name*) Head Teacher to protect unattended User equipment from loss, damage or theft both on-site and off-site;
- Comply with (*Insert system name*) ICT security and Back-Up Procedures: virus check the contents of all email messages used in conjunction with Insert system name and notify the Network Manager if you suspect any malicious code, e.g. viruses and Trojan horses;
- Ensure that any documents or magnetic media, or other removable media such as CDs, DVDs etc., you use are given the correct sensitivity labelling, and if necessary are registered and secured in an appropriate security container;
- Remember that it is a fundamental principle that knowledge or possession of sensitive information is to be strictly limited to those Users that have a need to know and appropriate privileges. (*Insert system name*)Users are to adhere to this principle;
- Comply with the (*Insert system name*) Acceptable Use Policy:
    - If you need an account on a (*Insert system name*) server you will need the approval of the (*Insert system name*) Head Teacher, or in their absence, the Network Manager. Once approved the Head Teacher will instruct the (*Insert system name*) Network Manager to have your account created; and,
    - You will need to notify the (*Insert system name*) Head Teacher if your access requirements change.
- Challenge anyone you do not recognise, if you are suspicious of that person report to the Institution office by the quickest means;
- Ensure that laptops are secured with cable locks when left unattended;
- Make sure that anti-virus software, and personal firewall software is installed, up to date, and active on laptops that you use for access to (*Insert system name*). For advice on correct configuration of laptops, contact the Network Manager;
- Comply with the (*Insert system name*) Password Policy

As a (*Insert system name*) User, you are NOT to:
- Make any changes to (*Insert system name*) without following the policies for change control;
- Load software (e.g. computer games) onto (*Insert system name*) equipment without prior consent of the network manager. or use it concurrently on workstations, while Insert system name sessions are open;
- Disable the anti-virus software resident on workstations or laptops;
- Test (*Insert system name*) security features or use any software or tools to examine the network or workstations without authority.
- Attempt to gain unauthorised access to (*Insert system name*);
- Attempt to use (*Insert system name*) under another identity (UserID) or share your password with anyone else'
- Attempt to access information outside of your normal access rights or duties. You will be responsible for all actions undertaken on (*Insert system name*) using your UserID;
- Disclose your password. You are to contact your administrator to change your password if your password has become disclosed or you are instructed to by the system.

Appendix D – Glossary of terms

Access Point (AP)	A wireless access point is a specially configured node on a wireless local area network (WLAN) that is designed to act as a central transmitter and receiver of WLAN radio signals. This allows any wireless device to connect to the WLAN via the AP.
Administration resources	Any digital resources that are used to maintain the administrative activities of an institute. This includes but is not limited to the institute's Management Information System (MIS)
Anti-virus software	Anti-virus (AV) software is used to scan email messages looking for defined viruses, which show up as known signatures that the software recognises as a virus. AV solutions must be implemented on each desktop and on the email gateway or email server function, where all incoming messages are scanned before being delivered to the recipient. Best practices for preventing viruses on a network call for both desktop and gateway or server AV to be implemented, to ensure that laptops that plug into the LAN cannot corrupt systems "behind" the AV Gateway. It is important that both types of AV software are kept up-to-date, as new viruses are found on a very frequent basis.
Applications	Computer programs designed for a specific task or use
Asset	Something which is of value and needs to be protected
Assurance	The confidence that may be held in the security provided by a system, product or process
Automated process	Any digital process that require little or no human input
Availability	Ensuring that authorised Users have access to information and associated assets when required
Bandwidth	Bandwidth in computer networking refers to the data rate supported by a network connection or interface. One most commonly expresses bandwidth in terms of bits per second (bps) or Mbps (millions of bits per second). Bandwidth represents the capacity of the connection. The greater the capacity, the more likely that greater performance will follow, though overall performance also depends on other factors, such as latency.
BS 7799	The British standard for ICT security management
Clampdown / Hardening	The method by which Users may be denied access to resources to prevent accidental or deliberate threat
Collaborative tools	Applications that enable several concurrent users to work in a common environment, allowing communication and integration of their work to achieve a shared goal
Confidentiality	Ensuring that information is accessible only to those authorised to have access
Configuration Control	A system of controls imposed on changing controlled objects including documentation
Curriculum resources	Any digital resources that are used to deliver curricular activities e.g. learning platforms and applications
Denial of service attacks (DoS)	A denial of service attack attempts to put the target site out of operation, frequently by flooding the site with bogus traffic, thus making it unusable. The attacker attempting to create a denial of service condition will oftentimes try to compromise many PC's, and use them to "amplify" the attack volume, and to hide his or her tracks as well. This is called a Distributed Denial of Service Attack (DdoS). Denial of service attacks are very hard to effectively protect against.
DHCP	DHCP allows a computer to join an IP-based network without having a pre-configured IP address. DHCP is a protocol that assigns unique IP addresses to devices, then releases and renews these addresses as devices leave and re-join the network.

DMZ	DMZ stands for De-Militarised Zone. In computer networking, DMZ is a firewall configuration for securing local area networks (LANs). In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet. One or more computers also run outside the firewall, in the DMZ. Those computers on the outside intercept traffic and broker requests for the rest of the LAN, adding an extra layer of protection for computers behind the firewall.
e-GIF – e-Government Interoperability Framework	This is the set of standards for e-gov which will become mandatory. Includes accessibility and usability, XML compliance and use of metadata. The two parts of the latest version can be accessed from: http://www.govtalk.gov.uk/schemasstandards/egif.asp
Ethernet	Ethernet is a physical and data link layer technology for local area networks (LANs) that follows the 802.3 family of standards.
Exploits	When vulnerabilities are found in software, the hacker community will frequently attempt to develop attack code that takes advantage of the vulnerability. This attack software is called an exploit, and exploit code is frequently shared among hackers, as they attempt to develop different sophisticated attacks. The speed with which these exploits are developed is becoming ever faster. The current record is 8 days from announcement of the vulnerability to a proven exploit being released on the internet.
Firewall	A network firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal local area network against malicious access from the outside.
FITS	Framework for ICT Technical Support – http://www.becta.org.uk/fits/
FTP	FTP stands for File Transfer Protocol and is a protocol designed to allow the transfer of files via IP networking.
Functional Specification	Document that describes in detail what a product must deliver in terms of form, fit, function and performance to satisfy the intended use.
Gateway	A network gateway is an internetworking system, a system that joins two networks together. A network gateway can be implemented completely in software, completely in hardware, or as a combination of the two.
Gateway	A device on a network that serves as an entrance to another network. In Institutions, the gateway is the computer/device that routes the traffic from a workstation to the outside network that is serving the Web pages. In homes, the gateway is the ISP that connects the user to the internet
H.323	An International Telecommunication Union (http://www.itu.int/) standard defining how audio and visual conferencing data is transmitted across networks.
Hop	In computer networking, a hop represents one portion of the path between source and destination, usually defined by being between two devices.
HTML – Hypertext Markup Language	A mark-up language used to create web pages. Various instructions and sets of tags are used to define how the HTML page will look.
ICT security Policy	The set of laws, rules and practices that regulate how assets, including sensitive information, are managed, protected and distributed
Identification & Authentication	The process used to determine and verify a User's identity; usually consisting of a userid and a password
IETF	Internet Engineering Task Force; the main standards organisation for the Internet
IMAP	Internet Message Access Protocol; an email server that sends a copy of a message to a client while retaining the original message on the server
Infrastructure	The physical resources forming the institution's network
Institution	A place of learning where ICT is being used. In this document this includes all schools but is not necessarily limited to the school sector e.g. could include Adult Learning institutes
Integrity	Safeguarding the accuracy and completeness of information and processing

	methods
Intrusion detection/prevention systems	Intrusion Detection (IDS) and intrusion prevention (IPS) Systems are products that can analyse certain types of traffic, and determine whether the traffic is legitimate traffic, or if the traffic matches a known pattern indicating that it is an attack. An example might be web (port 80) traffic, which a firewall would typically be configured to allow. An IDS system can look at the traffic, and determine that the traffic is actually an attack, and not valid User traffic, based upon the pattern. An IDS product will provide an alert if there is invalid traffic, while an IPS product will block the offending traffic.
IP	IP, which stands for Internet Protocol, is the world's most popular network protocol. Data travels over an IP-based network in the form of packets; each IP packet includes both a header (that specifies source, destination, and other information about the data) and the message data itself.
IP Addresses	An IP address is the logical address of a network adapter. The IP address uniquely identifies computers on a network. An IP address can be private, for use on a LAN, or public, for use on the Internet or other WAN. IP addresses can be determined statically (assigned to a computer by a Network Manager) or dynamically (assigned by another device on the network on demand).
L2TP	Layer Two (2) Tunnelling Protocol; an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks
LA	Local Authority. Either the Local Education Authority (LEA) or the Local Education Partnership (LEP) or a similar organisation.
LAN	A Local Area Network (LAN) supplies networking capability to a group of computers in close proximity to each other. A LAN is useful for sharing resources like files, printers, and applications. A LAN in turn often connects to other LANs, and to the Internet or other WAN (Wide Area Network).
Learning platform	'Learning platform' is a generic term covering a variety of different products, all of which support online learning in some way and includes delivery via intranets, via the internet and third party hosting. Learning platform capabilities can vary from systems that provide bespoke learning content or access to third party content only, to systems which provide communications, assessment, tracking and MIS interoperability facilities.
MAC	Media Access Control (MAC) is an addressing and access control protocol that works at Layer 2, and provides routing to IP protocol.
Network	The institution's infrastructure, applications, services and data
OpenDocument	OpenDocument is a freely available document format specification approved as an OASIS standard and recommend by the European Union for standard file formats and document interchange. The file extensions are .odt for text documents, .ods for spreadsheets, .odp for presentation programs, .odg for graphics and .odb for database applications.
Phishing	Phishing is the act of sending an email to a User, falsely claiming to be an established legitimate organisation, e.g. your own bank, in an attempt to scam the User into surrendering private information that will be used for identity theft. The email directs the User to visit a web site, which is a physical copy of the legitimate site, where they are asked to update personal information, such as passwords, credit card and bank account numbers that the legitimate organisation already has. The web site, however, is bogus and set up only to steal the User's information.
POP3	A POP3 (Post Office Protocol) email server receives email and sends the entire message upon a client's request. Once received, the message is no longer stored on the server unless specifically instructed to keep a copy.
Port	In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is
PPP	Point-to-Point Protocol; a method of connecting a computer to the Internet
PPTP	Point-to-Point Tunnelling Protocol; a technology for creating Virtual Private

	Networks (VPNs)
RBC – Regional broadband consortium	Regional broadband consortia (RBCs) are consortia of LAs that were originally established to procure cost-effective broadband connectivity for institutions and to promote the development of content for broadband networks. They link to form a National Education Network. (http://broadband.ngfl.gov.uk)
Remote locations	Any location that is outside of the actual institution network e.g. the student's home.
Repository	A computer resource which is dedicated to storage of curriculum and/or administration data.
Risk	The likelihood of a threat occurring and being successful in exploiting a vulnerability and causing a breach of security
Routers	Routers are perhaps not generally thought of as "security solutions", however most routers today provide packet filtering capabilities, and they can be used to enhance the security of networks. In addition, there are certain security tasks that are best performed on the router in order to optimise the performance of the overall network, and to reduce the processing load on a firewall.
Security	A combination of confidentiality, integrity and availability considerations
Services	Functional deliverables derived from a particular application, typically provided over a network to users.
S-HTTP	An extension to the HTTP protocol to support sending data securely over the World Wide Web
SIP	Session Initiation Protocol; an Internet Engineering Task Force (IETF) protocol and proposed standard for real time multimedia interaction, such as videoconferencing and instant messaging
Smartcards	A smartcard is basically a plastic card (like a bank card, store card, membership card) with an embedded microchip and / or barcode. The microchip can be used for storing information and providing authentication about identity.
SMTP/MIME	Simple Mail Transfer Protocol defines the message format and the message transfer agent which stores and forwards email. MIME is an encoding method that enables executable programs and multimedia files to be transported with email messages.
Spam	Spam is generally regarded as electronic junk mail. Some people define spam even more generally as any unsolicited email. Real spam is generally email advertising for some product (often bogus) or website containing unsuitable content sent to a mailing list or newsgroup. In addition to wasting people's time with unwanted email, spam also eats up a lot of network bandwidth. Spam is not a security threat as such, but spam techniques are increasingly being used to deliver malicious software. Spam can also be used to launch "phishing" attacks, which attempt to elicit confidential personal information (bank account information, credit card information, etc.) as a means to steal identity, or cause financial harm.
Spam filtering	Spam filtering can be implemented on the email server, or on a separate appliance sitting between the Internet and the mail server. There are many techniques that can be used to try and identify Spam, and generally the goal is to eliminate as far as possible false positives (legitimate mail misclassified as Spam), while also eliminating false negatives (Spam that slips past the Spam filter).
Spyware	Spyware is any computer technology that aids in gathering information about a person or organisation without their knowledge. On the Internet (where it is sometimes called a spybot or tracking software), spyware is usually a clandestine computer program installed onto a computer to secretly gather information about the user and relay it to advertisers or other interested parties.
SSL	Secure Sockets Layer, a protocol developed for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection

SyOps	Security operating procedures – The rules with which persons must comply in order to use a system as intended
TCP	Transmission Control Protocol; TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent
Threats or attacks	A direct security threat or attack is one aimed at a single Institution, e.g. an individual attempting to hack into an Institutions' network. A mass attack is usually a virus or worm, that is launched onto the Internet, which replicates itself to as many systems as possible, as quickly as possible. Attacks may come from inside or outside of an Institution.
Trojan horses	As the name implies, these are software programs that are put onto target systems (whether by a direct hack, or as the result of a virus or worm) that have a malicious intent. The Trojan lurks in the background without being detected. It can capture passwords, credit card and bank data or provide root access to the system remotely so that a hacker can take remote control of the PC for their own purposes.
UDP	User datagram protocol; a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network
Virtual Private Networks	A virtual private network (VPN) is a network that is constructed to allow secure communications over public communication lines to connect institutions and mobile Users. There are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorised Users can access the network and that the data cannot be intercepted or altered.
Viruses	Viruses are generally spread via email messages. Users unknowingly cause the virus to execute as a program on their system when they click on an attachment that runs the virus program or with some, just open the email to read it. Virus writers go to great lengths to disguise the fact that the attachment is in fact a virus. They also attempt to spread the virus by using the victim's address book to spread the virus further.
VLANs	A logical area in a computer network where any computer connected to the computer network can directly transmit to any other in the domain without having to go through a routing device.
VoIP – Voice Over Internet Protocol	Any technology providing voice telephony over IP (internet protocol). Basically using the internet for phone calls rather than the existing public phone system.
Vulnerabilities	Vulnerabilities are known (or newly found) security holes that exist in systems and software. In its broadest sense, the term 'vulnerability' is associated with some violation of a security policy. This may be due to weak security rules, or it may be that there is a problem within the software itself. In practise, all computer systems have vulnerabilities; whether or not they are serious and need to be addressed depends on whether or not they are likely to be used to cause damage to the system.
W3C - World Wide Web Consortium	An international consortium of companies involved with the internet and the Web, whose purpose is to develop common standards for the evolution of the World Wide Web. It is the chef standards body for HTTP and HTML.
Worms	A worm is a program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down. An example of a worm is the Blaster worm, which rapidly spread through the Internet in August 2003. The Blaster worm targeted Microsoft based computers and used a vulnerability in their operating systems.

WWW	The world wide web, commonly known as the Internet
XML - eXtensible Markup Language	XML is a mark up language which has two powerful features. It can be used to create other mark-up languages and it is software and hardware independent. This means if system A uses database X and system B uses database Y, they can exchange and share data if they both also make use of XML.

Appendix E – Collated Design Criteria checklist

1. Local Area Networks in institutions

Wired Networks

- Institution networks ***shall*** be of a star/tree design
- Institution networks ***shall*** use managed switches
- Institutions ***shall*** implement an Ethernet based wired solution as their primary network.
- Institutions ***shall*** install 802.3ab or 802.3z Ethernet in their backbone, between their servers and key network hardware.
- Institutions ***should*** install 802.3ab or 802.3z Ethernet (Gigabit Ethernet) in new builds or when upgrading their current network.
- The network ***shall*** be cabled with fibre optic cable or Cat5e or Cat6 copper cabling.
- Any copper cable ***should*** be rated to at least 350Mhz to ensure data integrity at high data rates.
- Installed cable ***shall*** have the ability to support data rates of up to 1Gbit.
- Where fibre is used for longer spans it ***should*** be single-mode.
- Where single mode fibre is used it ***should*** be 8.3/125 micron fibre.
- Where multimode fibre is used it ***should*** be 50/125 micron fibre.
- Cat3 or Cat5 ***shall*** be replaced with Cat5e or Cat6 or fibre optic cable.
- Institutions ***shall*** have NICs that support at least 100Mbps in every device connected to the wired network.
- Institutions ***should*** implement 1000Mbps NICs for all new devices connected to the wired network
- Public IP addresses ***shall*** only be allocated to outward facing devices (normally the institution's router).
- IP addresses ***should*** be allocated by the institution's RBC or LA.
- Institutions ***shall*** use DHCP for IP address management in accordance with any LA, RBC or national addressing scheme.
- NAT ***should*** be applied at LA level [58]

Wireless networking

- Wireless networking equipment ***shall*** conform to the IEEE 802.11a/b/g standards.
- New wireless networking equipment ***shall*** conform to IEEE 802.11a or 802.11g standards.
- Wireless networks ***shall*** be secured as set out in section 3.4.2.

Connecting multiple buildings

- Where device usage is high or in excess of 10 devices are to be networked, cable ***should*** be used wherever possible.
- If distances between buildings is less than 100m:
    - Optical fibre ***should*** be considered.
    - Duct shielded Cat6 cabling or fibre **may** be installed.
- For distances between buildings of 100m to 200m:
    - Optical fibre ***should*** be considered.
    - Duct shielded Cat6 cabling **may** be used in association with a repeater unit.
- For distances between buildings of greater than 200m:
    - Optical fibre ***should*** be used.

[58] It is important that the location of the network edge be examined when choosing how to implement NAT and DHCP, so that duplication of effort can be avoided. The NEN design document (http://www.becta.org.uk/NEN) contains advice on the best implementation of NAT by an LEA in order to ensure that their institutions are able to form a part of the National Education Network.

- Where device usage are low, or less than 10 devices are to be networked, and cabling is not possible/favoured:
    - 802.11a/g or Powerline technologies **may** be used.
- Where device usage is high or more than 10 devices are to be networked and cabling is not possible/favoured.
    - High bandwidth point to point wireless connections ***should*** be used.

Network type

- Institutions ***shall*** use a client/server network architecture.
- Institutions ***shall*** implement a repository with functionality for allowing mirroring of data and redundancy of physical media.
- Data ***shall*** be backed up at intervals as defined in Section 3.3.2.
- Institutions ***shall*** ensure that all new switches joined to the network are 802.1Q compliant (see 1.5.1 Class of Service (CoS))
- Institutions ***should*** replace older switches and hubs with managed 802.1Q compliant switches.

Fat Client Networks

- The centralised data repository ***shall*** reside on the network backbone unless it is held outside the institution.
- A secure link ***shall*** be provided to the central repository.
- Data rates between the central repository and the institution ***should*** be no slower than 100Mbps.
- Where data rates between the central repository and the institution are lower than 100Mbps, then a caching repository ***should*** be implemented at the institution.

Thin client Networks

- Full thin client implementations ***shall*** be capable of providing all apps and services as defined in chapter 2.
- Where thin client implementations are unable to provide all apps and services as per chapter 2, then it ***shall*** only be used in conjunction with fat client.

Peer to Peer Networks

- Institutions using peer-to-peer networks ***shall*** configure devices so that devices gain static or OS defined IP address if/when DHCP fails
- Institutions using peer-to-peer networks ***should*** ensure any data is synchronised with main network on a daily basis

Prioritising traffic

- Institutions using CoS ***shall*** detail a table of priorities so that their CoS policy is easily understood.
- Classification of applications ***should*** be limited to a select few applications so traffic priority can be provided with clearly discernible results.
- Institutions ***should*** implement Diffserv with DSCP as their first choice CoS strategy.
- Institutions ***shall*** consult with their LA, RBC, and service providers to ensure that QoS is implemented in a manner conducive to end-to-end delivery.
- Institutions ***shall*** ensure that SLS are in place if they are implementing QoS.

Flexible access

- Institutions ***shall*** give due consideration to implementing web interfaces for RAS, and ***should*** refer to Becta's ongoing work in this area.
- Institutions using web interfaces ***shall*** use SSL and/or S-HTTP to secure their web interface.
- Institutions ***shall*** not use dial-in solutions as their primary method of remote access.

- Institutions ***shall*** only implement a VPN solution if they are able to sustain support for the users as the user bases increases.
- Any VPN solutions implemented by institutions ***shall*** be based around internationally ratified standards for communication and security.
- Institutions ***should*** enable synchronisation between appropriate network data and portable devices.

2. Services and applications in institutions

Standards for applications used in institutions

- Pedagogical and administrative applications ***shall*** support open standards that allow the import and export of data in a range of commonly used formats that are independent of a particular platform.
- All educational applications ***shall*** provide an interface that is designed or can be tailored to suit the age and ability of the learners.
- Documents and data which are intended potentially to have a long lifetime ***should*** **not** be saved to proprietary file formats.
- Where only proprietary standards are available, strategies ***should*** be provided for migrating to open formats if and when they become available.
- Applications used in institutions ***should*** be designed for network installation.

Standards for office productivity applications

- Text document applications used in institutions ***shall*** provide the functionality to create, edit, save and print documents in open standard file formats.
- Spreadsheet applications used in institutions ***shall*** provide the functionality to create, edit, save and print spreadsheet files in open standards file formats
- Database applications used in institutions ***shall*** provide the functionality to create, edit, save and print database files in open standards file formats.
- Presentation applications used in institutions ***shall*** provide the functionality to create, edit, save and print presentation files in open standards file formats.

Standards for accessing web based content

- Browsers used in institutions ***shall*** be able to display websites using W3C standards.
- Browsers used in institutions ***shall*** allow the installation and use of third party plug-ins.
- Institutions ***shall*** use a content filtering system that ***should*** be managed by LAs/RBCs in discussion with institutions.
- Filtering ***should*** be able to be refined at an institutional level.
- Filtering solutions ***should*** include the use of traffic logs, the display of an onscreen message indicating a site has been blocked, the ability to block sites, and where appropriate, in accordance with user policies, to unblock particular sites.
- Internet access ***should*** be via a Becta Accredited ISP[59] or an ISP that provides the same or similar level of service.

Standards for creating web based content

- Institution domain names ***shall*** be in the format school.area.sch.uk[60]
- Website content produced by or for institutions ***shall*** be written using W3C standards (such as HTML v4.01, XHTML v1.0, CSS, XML or XSLT).
- All institution websites ***should*** conform to level 'Double-A' standard, as defined in the Web Accessibility Initiative (WAI - http://www.w3.org/wai) Web Content Accessibility Guidelines.

[59] http://ispsafety.ngfl.gov.uk
[60] See http://www.nominet.org.uk/SecondLevelDomains/AboutSecondLevelDomains/schuk/schuk.html

Standards for multimedia

- Proprietary file formats ***should*** be saved to only when an application is freely available for all workstation platforms via web download.
- Institutions ***shall*** provide applications with the functionality to create, edit, save and print still image files in open standards file formats.
- Media players used in institutions ***should*** support at least MPEG layer 3 (.mp3) or Ogg Vorbis (.ogg) for audio representation and MPEG layer 1 (.mpg) for coding moving pictures and associated audio.
- Animations developed by or for institutions ***should*** be saved and viewed in a freely available format.
- Vector graphics developed by or for institutions ***shall*** be saved in open standard file formats.

Learning platforms[61]

- Learning platforms that are accessible using web interfaces ***shall*** use SSL and/or S-HTTP to secure their web interface.
- The IEEE Standard for Learning Object Metadata ***should*** be used to describe learning materials.
- The IMS Question and Test Interoperability Specification ***should*** be used to write and describe assessment materials (questions or tests).
- Becta's Packaging and Publishing Learning Objects: Best Practice Guidelines[62] ***should*** be followed for the description, structure, and location of online learning materials.
- The IMS Learner Information Packaging Specification ***should*** be used when developing Learner Information systems.
- The AccessForAll Meta-data (AccMD) specification ***should*** be used to identify resources that match a user's stated preferences or needs. These preferences or needs ***should*** be declared using the IMS Learner Information Package Accessibility for LIP specification.

Communications

- Institutions ***shall*** ensure that all communications software purchased or developed for the institution uses recognised open standards.
- Institutions ***shall*** consult with their RBC or LA before purchasing H.323 video conferencing equipment.
- Institutions ***shall*** use an H.323-aware Firewall/NAT device or H.323 Proxy (this ***may*** be at the LA or RBC level).
- Institutions ***shall*** register with the Janet Videoconferencing Service (JVCS)[63].
- Institution ***shall*** use the National Education Network for H.323 video conferencing.
- Institutions ***shall*** arrange Quality Assurance Assessments via JVCS for all room-based video conferencing endpoints.
- Institution H.323 endpoints ***shall*** only accept external calls (those originating from outside of their RBC) from JVCS.
- Technical support with videoconferencing network problems, such as those caused by firewalls, ***shall*** be sought from RBCs, Local Authorities or their approved support centres.
- Institutions ***shall*** consult with their LA before purchasing VoIP solutions.
- If replacing existing PBX systems then institutions ***should*** implement VoIP solutions
- H.323 and SIP systems ***may*** need to be configured to traverse firewalls.
- Email products used in institutions ***shall*** support interfaces that conform to SMTP/MIME for message transfer
- Email products used in institutions ***shall*** as a minimum conform to POP3 for remote mailbox access

[61] Institutions are strongly encouraged to wait for Becta's Learning Platform functional specification to be published before purchasing a Learning Platform.
[62] http://www.becta.org.uk/page_documents/industry/content_packaging.pdf
[63] Janet Videoconferencing Service – http://www.jvcs.video.ja.net/

- Where additional mail facilities are required, email products that provide advanced mail access facilities ***shall*** conform to IMAP for remote mailbox access
- Mailbox access via a web browser ***shall*** use HTTPS or secure VPN
- Institutions ***shall*** use an email filtering system that ***should*** be managed by LAs/RBCs in discussion with institutions.
- Filtering ***should*** be able to be refined at an institutional level.
- Internet access ***should*** be via a Becta Accredited ISP[64] or an ISP that provides the same or similar level of service.

Access to content

- Where users will not necessarily have access to the same computer at all times, IMS ACCLIP ***should*** be used to facilitate transferable user customisable interfaces.
- Institutions ***should*** use a caching system and this ***shall*** be as described in Becta's Caching & Content Pre-positioning Technical Paper[65].
- Frequently accessed media rich, static content ***should*** be located as close as possible to the users, such as in the institution.
- Infrequently accessed or frequently changing content ***should*** be located at a central location (or small number of mirror locations), such as at the LA or RBC.
- Institutions ***should*** consider implementing location based services.
- Institutions ***may*** enable users to print to their nearest printer.
- Institutions **may** provide custom desktops suited to a particular scenario (such as their location or subject area).

Collaborative learning tools

- If implemented, IM solutions ***shall*** allow for real time text exchange and presence services.
- If implemented, IM ***should*** be managed, secured, and monitored.
- Blogs ***should*** allow for hyperlinking, trackbacks and comments.
- Blogs ***should*** have the ability to be managed and secured, allowing only authorised bloggers to post messages.
- Institutions ***should*** consider their design and choice of wikis to allow granular access control over the editing of pages.
- Where institutions make 'news' available on their web site they ***should*** also make an RSS feed available.
- Institutions ***should*** ensure their RSS feeds conform to RSS 1.0 specification[66].

Minimising administration

- Institutions ***shall*** install Common Basic Data Set (CBDS) compliant MIS software[67].
- Institution MIS systems ***should*** be client platform independent.
- Institution MIS systems ***should*** link in to their learning platform[68].
- Institution MIS systems ***should*** include the functionality to address the following:
    - Pupil Records
    - Staff/Personnel Management
    - Curriculum Planning
    - Timetabling and Options Planning
    - Staff Cover
    - Pupil Attendance and Behaviour
    - Assessment and Performance
    - Examination Management

[64] http://ispsafety.ngfl.gov.uk
[65] http://www.becta.org.uk/nen
[66] http://purl.org/rss/1.0/spec
[67] Compliancy is confirmed by the relevant supplier signing the MIS Interoperability Agreement. More information about this Agreement, can be found at www.becta.org.uk/mis.
[68] See 2.6 Learning platforms

  - Special Educational Needs
  - Financial Management
  - Property and Equipment Management
  - Payroll and BACS
- Each of the above business processes ***should*** be able to share data seamlessly between each other irrespective of whether each module is from the same supplier or not.
- Institutions ***should*** implement an electronic facilities management system.
- Where institutions implement a smartcard system, smartcards ***shall*** conform to the e-GIF specifications as described at http://www.govtalk.gov.uk/egif/eaccess.asp#table11a.

E-portfolios

- Institutions ***shall*** provide learners with access to electronic portfolios[69].
- Institutions ***shall*** only implement components of e-portfolios that are proven to interoperate with one another.
- Institutions ***shall*** consult their LA/RBC before investing in e-portfolio solutions.

3. Implementation of ICT security in institutions

ICT security policies and procedures

- Institutions ***shall*** produce a short easily understood and realistic ICT security policy.
- Institutions ***should*** produce System Operating Procedures.
- Adult users and guests of institutions ***should*** sign to indicate their agreement with the procedure.
- Educators ***should*** encourage learners to adopt the practices.

Physical security

- Sensitive material ***shall*** not be left unattended or unsecured.
- Sensitive information sent to printers ***shall*** be removed from the printer immediately.
- Workstations ***should*** be password protected when left unattended, unless the area has been physically secured.
- Padlocks/equivalent controls **may** be used to protect workstations and laptop computers. This includes workstations that are built into desks or are physically bolted/secured to furniture and Kensington locks for laptops.
- Procedures ***shall*** be developed to record all devices and software in a detailed ICT resource register.
- The register ***shall*** record the location of a device plus key information, for example, serial number, description, change of use, owner, configuration etc.
- The register ***shall*** record software (including relevant license key, version number, etc) installed upon that device.
- The register ***shall*** record software patches and security updates installed on individual devices.
- Regular audits of equipment ***shall*** take place.
- Overall audit responsibility for the register ***should*** lie with a designated individual.
- Users ***should*** only take devices off-site with formal signed approval.
- Users ***should*** be given guidelines on the use and protection of the equipment when away from the institution.
- Devices which are regularly removed from institutions' premises, ***should*** be audited more frequently.
- Institutions ***should*** provide hardware redundancy for end user devices that are critical to learners.

[69] Becta and JISC are working together to develop a specification for e-portfolios. Developments will be posted at http://www.becta.org.uk when available.

- Critical equipment ***shall*** be protected by Uninterruptible Power Supplies (UPS), and ***should*** be tested regularly. Critical equipment ***may*** operate in failover or in redundant pairs.
- System configurations ***should*** be backed up and stored in a secure location and be the responsibility of the Network Manager.

Data security

- User ids ***should*** be changed when compromise is feared or suspected.
- Shared (as opposed to personal) User ids ***should*** only be used for the youngest of learners.
- Shared ids ***should*** be protected by as strong/complex a password as possible and ***should*** have limited privileges.
- Users ***should*** be as protective of their id as they would their password; if an attacker acquires your id, they then only have to crack your password to gain system access.
- A formal password policy ***shall*** be adopted by the institution.
- Passwords ***should*** **not** be written down.
- Passwords ***should*** **not** be based on personal information that can be easily accessed or guessed.
- Passwords ***should*** be a combination of letters, numbers, and special characters and ***should*** use both lowercase and capital letters.
- Shared passwords ***should*** be avoided but limited access privileges ***should*** be used where shared passwords are deemed essential/appropriate.
- Passwords ***should*** be changed frequently.
- Institutions ***shall*** have a backup strategy that includes details of what is backed up, the frequency of backup, storage of back up media (on and off site), recovery procedures, the person responsible for backing up data.
- The person responsible for back up ***shall*** be appropriately trained.
- Institutions ***should*** educate individual users on how to backup their own personal data that is not backed up centrally by the system.
- Users ***should*** only save work to local devices when that device is regularly synchronised or backed up via removable media.
- System backup operations ***should*** be performed on a daily basis and ***should*** be transparent to users.
- Tests ***should*** be performed at regular intervals to verify that data can be recovered from the system backup media.
- Institutions ***should*** perform daily backups of new or changed data complemented by a full weekly backup of:
    - All institution administrative data.
    - All users personal data stored in the network user folders.
    - All data stored in shared areas.
    - All changeable educational data stored on the network.
    - The mail server, or as a minimum, individual mailboxes.
    - Operating system/system state data.
    - All activity and audit log files.
- Media containing daily backups ***should*** be stored in fire proof safes wherever possible and full backups ***should*** be removed off-site to a secure location for safe-keeping.
- All devices, including stand-alone devices and portable ICT equipment, ***shall*** be protected by a recognised anti-virus (AV) package.
- The AV package ***shall*** provide an automatic update facility for virus definition files.
- The software ***shall*** be set to scan any new media detected or files received or opened by any route.
- Institutions ***shall*** ensure that AV packages are up to date and all devices have the most up to date virus definitions.
- All documents and removable media ***shall*** be subjected to an anti-virus scan prior to being transferred onto the Institution network.
- Users ***should*** be educated in the safe handling of any media used to transfer data from one system to another, e.g. floppy disks, memory sticks etc.
- Institutions ***shall*** have access to spyware protection software

- Institutions ***should*** implement hybrid systems for protection from spyware
- Scanning and removal of spyware ***should*** take place at regular intervals on all an institution's machines
- Institution users ***should*** be educated on the dangers and symptoms associated with spyware
- Institutions ***shall*** seek advice on regional firewall policy from their LA or RBC.
- Unnecessary network ports ***shall*** be closed and the default setting ***should*** be 'deny all'
- If an institution has its own firewall they ***shall*** liaise with their LA/RBC regarding firewall policy.
- Open network ports for normal network functionality ***may*** include; Port 25 – SMTP (mail); Port 80 – HTTP (internet access) and; Port 161 – SNMP (network and firewall monitoring).
- Personal firewalls ***may*** be used for devices used to access the internet from outside the control of the institution's network firewall
- Institutions ***should*** enable the logging of all the following events:
    - All logon attempts whether successful or not.
    - All logoff attempts whether successful or not.
    - Creation, deletion or alteration of access rights.
    - Creation, deletion or alterations of passwords.
    - Creation, deletion or alteration of system log files.
- Users ***should*** receive guidance in the importance of safeguarding media.
- Sensitive or valuable data stored on media ***should*** be removed as soon as possible.
- Media ***should*** be virus scanned on re-introduction to the system.
- Data stored on media ***should*** be synchronised or moved to the institution's repositories as soon as possible.

Network security

- Unused patch leads ***shall*** be removed from network equipment.
- Routing and switching cabinets ***shall*** be locked and all keys strictly controlled.
- Cables into institutions or between buildings ***should*** be located underground or be adequately protected from physical interference.
- Network cabling ***should*** be protected from unauthorised interception or damage by utilising wall cavities and behind walls wherever possible.
- Regular checks ***should*** be made to ensure that all cables are routed to their correct terminating equipment.
- Unused ports on network equipment ***should*** be disabled or physically taped over.
- Regular audits ***shall*** be carried out to ensure proper use of network equipment and associated software.
- Institutions ***shall*** change default settings of WLAN equipment.
- Institutions ***should*** give their WLAN networks a name (SSID) that cannot be associated with the institution.
- Institutions ***should*** disable SSID broadcasting.
- Institutions ***should*** employ regular intrusion detection checks.
- IP addresses for WLAN clients ***should*** be limited to the maximum number of devices that could realistically associate with that AP where DHCP and NAT is performed by the AP.
- Institution's ***should*** disable features that allow an AP to be administered via the WLAN.
- Institution's ***shall*** use as high a standard of authentication for WLANs as they do for their wired networks.
- Institution's ***shall*** use WPA encryption and ***should*** use WPA2/802.11i security where possible.
- Institution's ***should*** **not** use mixed mode in WPA.
- Institutions waiting to upgrade to WLAN equipment using WPA/WPA2 ***should*** authenticate individual devices via MAC address recognition or ***should*** consider using a separate network segment policed by a dedicated firewall.
- Institutions waiting to upgrade to WLAN equipment using WPA/WPA2 ***should*** limit access to sensitive data over the WLAN.

Internet and remote access security

- Institutions ***shall*** install a reliable virus scanner, which screens all incoming and outbound messages and attachments for email viruses and worms.
- A content checking tool ***shall*** be installed.
- An efficient anti-spam tool ***should*** be installed.
- A quarantining area ***should*** be implemented for dubious incoming and outgoing emails.

4. Network Technologies in institutions

Defining functions of the Edge

The Network *edge* is vital for communication with the outside world, and so;

- ***shall*** be connected directly to the network core.
- ***shall*** contain a means of communicating and routing network traffic to the correct locations.
- ***shall*** be adequately protected against any unauthorised attempts to access the institutions LAN from outside.
- ***shall*** have the ability to accept incoming traffic from authorised sources.
- ***should*** be equipped with a means of caching data, so that potential bottlenecks in educational traffic can be mitigated.
- ***should*** be able to filter web traffic based on URL (where it cannot, URL-based web filtering ***shall*** be implemented at the LA/RBC).

Universal functions for Edge equipment

- *Edge* equipment ***shall*** have secure management capability allowing alterations to be made to configurations of this equipment by authorised and authenticated administrators.
- Configuration profiles of the *Edge* equipment ***shall*** be able to be backed up.
- Security ***shall*** be addressed whether this is by the router or by a separate hardware or software firewall at institutional or regional level.
- All *edge* equipment ***should*** be protected by UPS equipment (see Core section for specifications for UPS equipment)
- Secure management capability ***should*** be available remotely as well as locally.
- There ***should*** be a gigabit connection between *edge* equipment and the LAN core

Edge Redundancy

- Redundancy ***should*** be provided for the key network *edge* equipment, whether that redundancy is provided by the institution having spare equipment or by a service agreement with a replacement clause. The primary concern is the router, allowing replacement of the unit in case of failure.
- Firewall configuration ***should*** always be backed up to allow fast reapplication of the policies if problems occur.
- Access to a backup firewall ***may*** be provided
- ISDN or ADSL backup ***may*** be provided and configured in case of router failure.

Routing Devices

- Routing devices ***shall*** support open standard routing protocols such as OSPF or IS-IS.
- Routing devices ***shall*** support standards based encapsulation (eg: PPP or PPPoE)
- Routing devices ***shall*** support DNS and be DHCP and NAT capable (see also 1.1.5).
- Routing devices ***shall*** support a minimum of 8Mbps/2Mbps for egress traffic (as per the DfES guidelines).
- Routing devices ***shall*** have upgradeable software based feature sets.
- Routing devices ***shall*** support multicast protocols.
- Routing devices ***shall*** support access control lists.
- Routing devices ***shall*** support the following QoS/Traffic management standards:
    - Differentiated Services (DiffServ) and MPLS (Multiprotocol label switching) for the QoS Service Model

  - Low Latency Queuing (LLQ) for Congestion Management
  - Differentiated Services Code Point (DSCP) for Classification/Marking
  - Diffserv-compliant Weighted Random Early Detection (WRED) for Congestion Avoidance
  - Traffic Control. Use Traffic Shaping and Policing i.e. Committed Access Rate (CAR)
- Routing devices ***should*** be scalable and modular to allow the addition of extra modules to increase the number of ports, provide additional modes of connectivity (such as adding fibre ports to a predominately ethernet provisioned router) and increase the amount of onboard memory, or similar.
- Routing devices ***should*** suffer minimal performance degradation when using QoS or data compression.

Firewalls

- Firewalls ***shall*** comply with the specifications given in section 3.3.5
- Firewalls ***shall*** also comply with the NEN design document security requirements

URL filters

- URL filters shall comply with section 2.3

Caching and Content Delivery

- Caching and Content delivery systems ***shall*** comply with section 2.8.1.
- Caches ***shall*** not be located in-line with the institution's broadband connection.

Defining functions of the Core

- The *core* ***shall*** enable the highest data rates within the institution, and ***shall*** ensure the integrity of network packets falls within locally defined tolerances.
- The *core* ***shall*** provide management opportunities and monitoring tools to ensure that high network performance,
- The core ***shall*** provide server functions for the institution, including, but not limited to, data storage, application services, and security management
- The *core* ***shall*** support CoS throughout.

.*Universal functions for Core equipment*

- Manageable *core* equipment ***shall*** have the capacity to be managed both directly and remotely
- Management services ***shall*** have access to them secured by a unique ID and password(see also 3.3.1).
- *Core* equipment ***shall*** support 802.1Q to enable priority queuing and VLAN functionality (see also 1.4.5).
- *Core* equipment ***shall*** support 802.1p priority queues for CoS support
- *Core* equipment ***shall*** be cascaded in a manner that ensures the speed and integrity of network packets is not adversely affected
- All *core* equipment ***should*** be protected by power management hardware

Redundancy

- Institutions ***shall*** have contingencies in place to enable the timely replacement of key *core* equipment.
- Backups ***shall*** be taken of the users files so that they can be restored in case of failure. The processes for this are covered in section 3.3.2.
- Institutions ***should*** implement network fault finding software, and ***should*** monitor the network

Switches

Core switches:

- ***shall*** be capable of full duplex and auto-sensing.
- ***shall*** employ store and forward, fragment free or adaptive switching
- ***shall*** have the capacity to be managed both directly and remotely
- ***shall*** support 802.1Q to enable priority queuing and VLAN functionality.
- ***shall*** support 802.1p priority queues for CoS support
- ***should*** have latency of no greater than 20 Microseconds for a 64-byte frame.
- ***should*** employ SMON as defined by RFC 2613
- ***should*** support Power over Ethernet as defined by 802.3af
- ***should*** be scalable and modular to allow expansion through the addition of extra modules.
- ***should*** be over-provisioned with ports to allow for future expansion of the network OR have the capability to provide this at a later date.

Servers

- Servers ***shall*** use dedicated server operating systems
- Servers ***shall*** be equipped to enable data backup locally or remotely (see also 3.3.2)
- Servers ***shall*** have processing power, RAM and storage sufficient to cope with all applications that an institution requires them to run.
- Servers ***should*** be connected to *core* switches with at least gigabit-rated NICs that support full-duplex operation.
- Servers ***should*** have disk redundancy features via RAID or similar

Server Operating Systems:

- ***shall*** provide a kernel, disk operations, and file management
- ***shall*** be network enabled
- ***shall*** provide user administration functions
- ***shall*** have administration functions protected by authentication techniques.
- ***shall*** be currently supported by the manufacturer or Distro.
- ***should*** provide logging of errors and access (see also 3.3.6)

Storage

- Where SANs are used, they ***shall*** use the iSCSI standard as defined in RFC 3720 or FCIP if a fibre channel solution is used
- Where SANs are used, they ***should*** be managed in accordance with ANSI INCITS 388-2004

Power management

- UPS systems ***shall*** carry the CE mark for electrical equipment.
- All UPS systems ***shall*** comply with UL1449
- All UPS systems ***shall*** also comply with the relevant IEEE standards from the 62 series
- UPS ***shall*** provide enough power to protect all mission critical *core* equipment for at least 10 seconds hold-up time.
- UPS systems ***should*** support SNMPv3 for management functions.

Management Tools

- Network management tools ***should*** support SMON.
- Network device management tools ***should*** use SNMPv3
- Network monitoring ***should*** use RMON for monitoring and management

Defining functions of the Core to the user device

The *core* to the *user device*

- ***shall*** provide a minimum of a 100Mbps rated connection to user devices when wired technologies are applied (see section 1.1.4)
- ***shall*** provide adequate network connections for all user devices in any given location, with the capacity for extra ports for future expansion.

Universal functions of Core to the user device equipment

- All cabled networking equipment ***shall*** be rated to at least 100Mbps. (see section 1.1.4)
- All equipment ***should*** be able to support 802.1Q. (see section 1.5)
- Any wireless LAN access points ***should*** be rated to provide signalling rates in excess of 50Mbps (although it is acknowledged that actual data rates will be much slower than this), and ***shall*** conform to the specifications set out in 1.2.

Redundancy

- Therefore this segment of the LAN ***should*** be monitored as a part of the ongoing *core* monitoring, and there ***should*** be a process in place to replace or repair faulty equipment in a time scale that will not disrupt an institutions functions unduly.
- Institutions ***should*** ensure that where network ports are located, those locations are over-provisioned with ports, to allow for expansion and replacement ***should*** faults occur. This ***shall*** also apply equally to switch ports.

Switches

Core to the user device switches:

- ***shall*** be capable of full duplex and auto-sensing.
- ***shall*** employ store and forward, fragment free or adaptive switching
- ***shall*** support 802.1p priority queues for CoS support (see section 1.5)
- ***should*** have the capacity to be managed both directly and remotely
- ***should*** support 802.1Q to enable priority queuing and VLAN functionality. (see section 1.5)
- ***should*** employ SMON as defined by RFC 2613
- ***should*** support Power over Ethernet as defined by 802.3af
- ***should*** be over-provisioned with ports, with the capacity to implement (through expansion of the switch or similar) additional ports or have the capacity to expand to provide this.

Defining Functions of the User device

- The user device ***shall*** provide a user interface (appropriate to the user) for an institution's users, allowing them to access and interact with their files, network resources and content held outside the institution (whether this be directly or through a caching system).
- ***should*** allow manipulation of text, images and video as well as providing an audio interface (see chapter 2)

Universal functions of User device Equipment

All network connected user device devices

- ***shall*** have the ability to view office productivity documents
- ***shall*** be equipped with a current version of a standards based web browser (see also 2.3).
- ***shall*** have a network interface able to transfer data at rates commensurate with the *Core* to the user device hardware serving the device.
- ***shall*** require authentication from an institution's user before granting access to secured areas of the LAN.

Redundancy

- Institutions ***shall*** ensure that user device devices are subject to a maintenance policy that ensures sufficient availability for the needs of the institution's users. This can be through the maintenance of a pool of replacement user device equipment, or service level agreements that ensure that faulty devices are fixed in a timely manner.

Accessibility

- Institutions ***shall*** ensure that access to user device equipment is available to all users irrespective of disability or special needs. Specialist equipment ***shall*** be managed in such a

way as to ensure that those users can access that equipment where and when they require it and that appropriate network services are available via that equipment

Workstations

- Workstations ***shall*** exceed the recommended specifications for the operating system and applications that they are expected to use.
- Workstations ***shall*** interface with the network at data rates of at least 100Mbps (see section 1.1.4).

Portable Devices

- Portable devices ***shall*** exceed the recommended specifications for the operating system and applications that they are expected to use.
- Battery life ***should*** exceed 1 ½ hours under full CPU load with full screen brightness.
- Laptops and tablet devices ***should*** have the appropriate ports or converters to allow them to connect to other equipment.
- Portable devices ***should*** include wireless networking capability.