Technical Principles for Institutional Technologies

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk
NOT PROTECTIVELY MARKED

page 1 of 1

Contents

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk
NOT PROTECTIVELY MARKED

page 2 of 2

Executive summary

The use of ICT in schools and colleges has moved from being an add-on to becoming fully integrated into teaching, learning and management. This means that the infrastructure technologies (ICT technical infrastructure, applications and services) for delivering and managing education must be reliable and secure and deliver an appropriate performance to meet the needs of the users. As technology advances and user needs change, there is a need to consider new and flexible ways to deliver this.

Well designed and maintained institutional technologies are key to an institution's ability to deliver a highly effective ICT resource to the learner, educator, managers and administrators.

It is Becta's aim to assist institutions strategically so they develop and maintain a coherent, sustainable and dependable ICT infrastructure, by offering guidance in specifying both the functional requirements for users and the technical principles that support delivery of those requirements, as well as offering procurement advice. To facilitate this, a common, standards-based approach needs to be taken to all areas of an institution's ICT infrastructure and services.

The overarching aim is to deliver *"Technology that works first time, every time for everyone, wherever and whenever they need it".*

A clear ICT vision will help to ensure that infrastructure technologies offer an ICT resource to the institution that is useful today and in future years. In addition, a clear information management strategy will help the institution to improve the quality of the data collected, and ensure that it is well managed and used more effectively to support teaching and learning, as well as ensuring that it is held securely and protected.

In this document, Becta addresses the technical principles that are needed in order to implement the ICT infrastructure to support requirements outlined in Becta's *Functional Requirements.*

Key technical design principles are covered in five areas: core principles, institutional infrastructure, connectivity, learning and management systems, and environmental sustainability. Each area has principles defined as either necessary or highly desirable if institutions are to support delivery of *Harnessing Technology for Next Generation Learning: Children, schools and families implementation plan 2009-2012* and *Next Generation Learning – The Implementation Plan for 2009-2012: Technology Strategy for Further Education, Skills and Regeneration.*

It is anticipated that the technical principles outlined here to support Becta's *Functional Requirements* will be achievable by all institutions yet allow for suppliers and advanced institutions to innovate and add extra value.

Introduction and overview

Introduction

This document defines the key ICT services and technologies to be deployed (or employed) within schools, colleges and other educational institutions in England. The principles are not exhaustive, because the local situation must reflect needs of users and because technology is continuously changing and evolving, but their use will help lead to infrastructure technologies that suit the demands of users within each individual institution, and that are reliable, sustainable, secure and flexible.

Institutions are increasingly making use of applications hosted outside the institution, using technologies such as virtualisation and cloud computing. Most, if not all, of the principles can also be applied in these scenarios, where there is an even more pressing need for clarity on levels of service and interoperability.

However technology changes and evolves, institutional infrastructures and services will always need to be based on the requirements of users. Learners and educators need easy access to high-quality resources to support them in their learning and teaching. Managers and administrators need to be able to use ICT resources that allow them to undertake their work efficiently and effectively.

Overview

In its *Functional Requirements*, Becta specifies a set of user requirements which will need a well developed institutional infrastructure. This paper describes the technical principles required in order to provide that institutional infrastructure and support the necessary functionality. In order to provide a useful document relevant to all stakeholders, this document is divided into the following sections:

    Section 1 – Core Principles

    Section 2 – Institutional Infrastructure

    Section 3 – Connectivity

    Section 4 – Learning and Management Systems

    Section 5 – Environmental Sustainability

It is expected that the technical principles, where appropriate, will be underpinned by open technical standards and specifications incorporating the work performed by many organisations such as BSI[1] and the IEEE[2] .

---

[1] http://www.bsi-global.com
[2] http://standards.ieee.org

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 manner. A standards-based approach will also help to ensure that interoperability between different institutions can be achieved. This is of paramount importance as learners become more mobile and require ever more integrated learning and management environments that are learner-centric rather than institution-centric.

Intended audience

This document has been written for a technical audience. Non-technical staff and institution leaders may find it more helpful to read the *Functional Requirements* document.

Wording conventions

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

- The word *shall* (italicised and bold) defines a principle that in Becta's view is essential in the delivery of ICT services
- The word *should* (italicised and bold) defines a principle that in Becta's view is highly recommended
- The word *may* (italicised and bold), means that the principle is optional, but should be considered.

In general the principles apply to all types of institutions. However, certain sector-specific principles may be cited, and these will be identified by prefacing the statement with the specific sector; for example, *Schools shall...*or *Colleges shall...*

The principles set out in this document are of two types:

- Design criteria (denoted by the �֡ symbol): these describe the detail of the infrastructure that should be in place
- Management approaches (denoted by the ⊞ symbol): these describe the management processes that should be followed to maintain the infrastructure, and should be considered in relation to Becta's Framework for ICT Technical Support (FITS).

1. Core Principles

In many cases remotely hosted services can offer more cost effective and environmentally sound solutions to infrastructure. However, interdependent services will need to have aligned service levels. For example, if the management information system is remotely hosted, institutions will need to ensure that the service level and bandwidth on their broadband line is appropriate.

Institutions have a responsibility to protect users, and as a minimum email and Web content must be filtered as appropriate.

Technical principles		
1a	An assessment *shall* be made to establish which core services are critical or have dependencies on critical services and appropriate service levels *shall* be put in place to ensure minimum disruption to overall service.	📈
1b	When aggregating services, particularly across multiple sites or institutions, consideration *shall* be given as to whether a remotely hosted service would be more cost effective and environmentally sound.	📈
1c	Email *shall* be filtered for inappropriate content.	📈
1d	Web content *shall* be filtered for inappropriate content.	📈

1.1 FITS

The Framework for ICT Technical Support (FITS) aims to support a reliable and effective infrastructure, by offering a structure to technical support and management tasks. It is therefore vital that institutions review their situation with regard to technical support and put in place a plan for the implementation of FITS. This is applicable regardless of whether the support is provided internally or is managed by an external resource.

Technical principles		
1.1a	Technical staff *shall* be offered the opportunity to become FITS accredited.	📈
1.1b	External technical support services *should* be purchased from organisations which provide FITS accredited staff.	📈

Version 1
March 2010
© Becta 2010
http://www.becta.org.uk
page 7 of 7
NOT PROTECTIVELY MARKED

1.2 Accessibility

The issue of making systems accessible for disabled users and those with a special educational need (SEN) is a legal, moral and ethical (not a functional) requirement.

All education providers are legally required to fulfil their obligations under Part 4 of the Disability Discrimination Act (DDA):

- An education institution should not treat a disabled person 'less favourably' for a reason relating to their disability.
- An institution is required to make 'reasonable adjustments' if a disabled person would otherwise be placed at a 'substantial disadvantage'.
- Adjustments should be 'anticipatory'.
- The legislation applies to all admissions, enrolments and other 'student services', which includes assessment and teaching materials.

Note: The DDA will be superseded by, and repealed after the introduction of the Equality Bill, which is due to come into force in Autumn 2010. It is anticipated that whilst the wording will change, the obligations will remain. See the Equalities Office [http://www.equalities.gov.uk/equality_bill.aspx].

Suppliers must ensure that their products enable institutions to meet their obligations to all learners, for example by ensuring that applications can be accessed and navigated using keyboard only control as well as a graphical user interfaces. Product design should recognise different modes of access and support hardware and software extensions, such as switches and screen reader software. The key point is that interfaces are adaptable and made easily accessible for a range of users with a range of needs.
Regional Broadband Consortia, FE colleges and training providers, and Local Authorities acting on behalf of institutions in aggregated procurements, will need to ensure that obligations for accessibility are met.

Educational institutions should be aware of anticipated needs as well as their existing obligations and needs of users, and how technology might support their strategies. Suppliers must demonstrate that they have an awareness of accessibility needs, and how they address these needs, which *shall* be embedded in an accessibility statement.

It is not expected that every tool, product and service will be completely accessible in every situation, but the accessibility statement *should* outline the scope and capacity to meet the diverse user needs of the learning population. This *should* cover individuals with a visual, auditory, physical, speech, cognitive, language, learning or neurological disability and *should* equally recognise the needs of an ageing population and speakers of an increasing diversity of languages.

The form of the accessibility statement should be simple to understand. Examples include the US Voluntary Product Accessibility Template, (VPAT) [http://www.itic.org/resources/voluntary-product-accessibility-template-vpat/].

It should be recognised that 'accessible' is not the same as 'usable', and accessibility should not be used as an excuse for poor design, and poor user experience.

Technical principles		
1.2a	Regional Broadband Consortia, FE colleges, training providers, and Local Authorities acting on behalf of institutions in aggregated procurements *shall* ensure that obligations for accessibility are met.	
1.2b	Institutions *shall* ensure suppliers have taken reasonable steps or can outline their willingness, capacity and capabilities to make reasonable adjustments to their offerings to meet accessibility needs or specific user requirements. The process by which such adjustments are to be requested and made must be clear, and where needs are not met, alternative methods *should* be made available.	
1.2c	A regular audit of services and provision *shall* be undertaken to identify current and anticipated accessibility needs of all users, including learners, parents, carers, staff and others. Every institution must have an accessibility plan and it must be published.	
1.2d	Suppliers *shall* outline the current capacity and capability of their goods and services to meet commonly identified user needs in an accessibility statement, or offer reasoned justification for lack of capacity and capability.	
1.2e	Suppliers *shall* ensure that products and services adhere to the principles underpinning the current W3C web content accessibility guidelines, which are technology neutral and can equally be applied to software, hardware, online tools and services: • Perceivable – information and the user interface must be presentable to users in ways they can perceive • Operable – the user interface and all components must be operable • Understandable – information and operation must be understandable • Robust – any device, system, service or information must be robust enough that it can be used and interpreted reliably by a wide variety of users and/or user agents e.g. assistive technologies	

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk
NOT PROTECTIVELY MARKED

page 9 of 9

1.3 Usability

Usability is the capacity of ICT services to be understood, learned, used and attractive to all user groups when used under specific conditions. It is about ensuring a service or tool is engaging and easy-to-use, has logical consistency, and maximises efficient working by minimising task time.

Technical principles		
1.3a	All user-facing services **shall** have undergone usability testing in accordance with best industry practice. Usability testing is best used in conjunction with user-centred design, a method by which a product is designed according to the needs and specifications of users, and service providers **should** be expected to demonstrate this.	

1.4 Inclusion

The issue of ensuring no users are excluded from accessing the opportunities provided is more subtle than implementing accessibility guidelines.

When using and implementing technology, schools, colleges, LAs and other institutions and agencies should aim to ensure that no groups or individuals are intentionally disregarded, by manifesting a culture of dialogue, openness and awareness, and by continually returning to the points of greatest challenge to constantly seek resolutions.

Technical principles		
1.4a	ICT implementation plans **shall** be demonstrably inclusive to ensure the benefits are applied to all users.	
1.4b	ICT services implementations **shall** be constantly reviewed to ensure no groups of users are excluded.	

1.5 Security management

Institutions must be confident that all resources in their ICT environment are protected from misuse, that users are protected from external parties trying to interrupt their daily use of the systems and be sure that users can only see information they should. Access to all systems must be properly classified, logged and auditable. For this to be achievable it is necessary to have a security management process that will ensure users are protected, and that the ICT environment and the data stored on it are as secure as possible. Security management is concerned with developing the techniques and managing the tasks that will allow institutions to do this.

NOT PROTECTIVELY MARKED

Technical principles		
1.5a	FITS security management or equivalent **shall** be implemented.	
1.5b	Information security management **shall** conform with current Cabinet Office and Becta's Data Handling Security guidance for schools and colleges (see 3.4a).	

1.6 Open Source software

The *UK Government ICT Strategy* supersedes but reinforces the principles of the previous *Open Source, Open Standards, Reuse Strategy*, published by the Cabinet Office [http://www.cabinetoffice.gov.uk/cio/ict.aspx]. Institutions must ensure that their own policies adhere to this. In order to offer best value for money, promote sharing and re-use and encourage innovation, it is vital that Open Source software solutions and services be considered by institutions.

Technical principles		
1.6a	Open Source solutions **shall** be actively and fairly considered alongside proprietary ones whenever new implementations are planned.	
1.6b	Where there is no significant overall cost difference between Open Source and non-open source products, Open Source **shall** be selected.	
1.6c	Suppliers **shall** provide evidence of consideration of Open Source solutions during procurement exercises – if this evidence is not provided, bidders **shall** be disqualified from the procurement.	

1.7 Hosted services

A hosted service is one that delivers a range or combination of ICT services and functions such as infrastructure, applications (including 'Software as a Service'), security, monitoring, storage, development, website hosting and email, over the internet or a wide area network. Hosted services offer a number of advantages over local or on-site hosting, including increased durability and reliability, consolidation of services, predictable recurring fees and costs and economies of scale. Infrastructure as a service refers to the supply and management of remotely or centrally hosted infrastructure.

'Remotely hosted' is defined as a service that is hosted and supported from outside the establishment purchasing the service.

'Centrally hosted' is defined as a service that is hosted within the establishment purchasing the service (such as a local authority), but that service is physically distributed to other establishments (such as a school).

Version 1
March 2010
© Becta 2010
http://www.becta.org.uk
NOT PROTECTIVELY MARKED
page 11 of 11

Technical principles		
1.7a	Consideration **shall** be given to the provision of services remotely via remotely hosted or centrally hosted services. Wherever possible services delivered to an institution **should** be delivered from remote or central host or hosts maximising the opportunities provided by an institution's broadband infrastructure. Data centres used **should** adhere to the Data Centre Code of Conduct.	⬚

1.8 Open standards

Open standards for interoperability are standards that are widely used, consensus based, published and maintained by recognised industry standards organisations. Open standards help enable interoperability of systems and applications; without open standards and interoperability, systems that operate using a myriad of formats, fields, data elements and transport methods will make the combination of data from different sources an exercise in frustration, resulting is users expending time, effort and ultimately money with data conversion, 're-keying' or simply scrapping the work and duplicating it by gathering the data all over again. Put simply, without interoperability, based upon open standards, systems will have limited abilities to share data, information and resources and many of the benefits of using ICT services will be correspondingly limited.

Technical principles		
1.8a	Suppliers **shall** adopt and implement open standards and this **should** be a requirement in all procurements.	⬚

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk

NOT PROTECTIVELY MARKED

page 12 of 12

2. Institutional Infrastructure

A well designed and maintained infrastructure is key to an institution's ability to deliver a highly effective ICT resource to all users. In order for the ICT infrastructure to be sustainable, flexible and adaptive, a common approach needs to be taken to network design, ICT resources and security. A clear standards-based approach will help to ensure that infrastructures offer an ICT resource to the institution that is useful today and in future years. It is expected that infrastructure implementations will adopt commonly used technical standards.

It is acknowledged that the majority of institutions will wish to implement or upgrade their infrastructure in a phased manner. As they do this, it is important that institutions recognise that alterations to one aspect of their infrastructure can have an impact elsewhere. It is also important therefore that an action plan is produced to allow the upgrade, replacement and installation of systems and equipment to occur in such a way that disruption to institutional functions is minimal.

Technical principles		
2a	A full infrastructure survey **shall** be conducted prior to major changes to institutional infrastructure. Attention must be paid to enabling the institution to meet its obligations under the Disability Discrimination Act, Equality Act and other relevant legislation.	
2b	Where major changes are planned, an action plan outlining the changes to be made to the infrastructure **shall** be produced, with full consideration of their impact upon the institution and other areas of the infrastructure.	
2c	A contingency plan **should** be available for rollback to known good service levels in the event that a new installation fails or cannot be made to work during the initial implementation window.	

2.1 Network management

Without proper management tools and processes in place, increasingly complex institutional networks can become impossible to administer; bottlenecks and faults can proliferate and services can degenerate. It is vital that an institution has in place the correct procedures to avoid this. Through careful management the common risks associated with complex networks can be avoided.

Technical principles		
2.1a	Network management and control **shall** be undertaken in accordance with FITS processes. This **should** be undertaken by an accredited FITS technician.	
2.1b	An up-to-date network diagram **shall** be maintained.	
2.1c	Network diagrams **shall** include information about network hardware, cable type, data rates, and include both wired and wireless network segments.	

2.1d	Wired networks *shall* be clearly labelled at patch panel and network access point and the patch panel *shall* be in a secured area or locked cabinet.	⚒
2.1e	Network management software *shall* be implemented.	⚒
2.2f	Regular network performance reports *should* be produced for senior managers. The reporting may include particular end-user-facing services, as well as the network as a whole.	📈
2.2g	Contingencies *shall* be in place to enable the timely replacement of critical network equipment.	📈
2.2h	Contingency plans to ensure continued business operation in case of systems failure *shall* be in place.	📈
2.2i	Network fault-finding software *should* be in place, and the network *should* be monitored.	⚒

2.2 Wired networks

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

Wired networks have become the industry standard because of their superior data rates, low cost and high degree of stability, with wired networks ubiquitous in education as the fundamental technology underpinning local area networks (LANs). A wired network *shall* therefore be used as the main network in an institution. Wireless networking *may* provide an additional layer of flexibility to enhance wired networks

Network topology

The topology of a network describes its physical or logical shape. Network topology is key to the efficient operation of the network and becomes more important as higher demands are placed on the network by bandwidth-intensive applications such as video conferencing.

Designs

With the increasing demands placed on the network from multimedia applications, a well-designed network is becoming ever more important.

Wired networks must be constructed in a resilient configuration so that they are not affected by the loss of one or more nodes in the network, giving better resilience and greatest availability.

Every device in the network must be served by a managed switch, which enables multicast (i.e. communications between a single sending computer and multiple receiving computers) and provides a more robust model in case of faults. This means, for example, if network segment A has a problem, network segments B, C and D can still function. Unmanaged switches and hubs can hamper the resilience of the network and must be replaced.

Technical principles		
2.2a	Institution networks *shall* be of a resilient design.	⚒
2.2b	Institution networks *shall* use managed switches.	⚒

Cabling

In order to facilitate a robust and reliable network, cabling must also be robust and reliable. Records must be kept showing the routing of all cables, and those cables must be supported by a warranty. Prior to installing cabling, an asbestos survey for the building must be checked and any measures necessary taken.

Technical principles		
2.2c	Networks *shall* conform to TIA/EIA standards for cabling.	⚒
2.2d	Cabling *shall* be supported by a manufacturer's warranty.	⚒
2.2e	A cable routing diagram *shall* be produced when the cable is first installed, and *shall* be kept up to date with any additions or changes.	⚒

Data rates

Data rates offer an indication of network performance, allowing institutions to gain a rough idea of the capabilities of their network equipment and cabling. Whilst in practice actual data rates will rarely correspond with the rated performance of equipment, the rated performance rates are indicative of real world performance and therefore can provide useful baselines.

Version 1
March 2010
© Becta 2010
http://www.becta.org.uk
NOT PROTECTIVELY MARKED
page 15 of 15

Technical principles		
2.2f	All wired network equipment *shall* support a minimum 100Mbps data rate.	
2.2g	All cabling *shall* support a minimum 1Gbps data rate.	
2.2h	Switches used in the backbone of wired Ethernet implementations *shall* support a minimum 1Gbps data rate across all ports.	
2.2i	The network backbone *shall* enable the highest data rates within the institution and *shall* ensure that the integrity of network packets falls within locally defined tolerances.	

Class of Service and Quality of Service

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, CoS technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a 'best effort'.

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. Quality of service is therefore the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. It is important though to make sure that providing priority for one or more flows does not make other flows fail.

Technical principles		
2.2j	Where CoS is implemented, a table of priorities *shall* be established to ensure that the CoS policy is easily understood.	
2.2k	Classification of applications *should* be limited to a select few applications so that traffic priority can be provided with clearly discernible results.	
2.2l	LAs, RBCs and service providers *shall* be consulted to ensure that QoS is implemented in a manner conducive to end-to-end delivery.	
2.2m	Service-level specifications *shall* be in place if implementing QoS.	

Version 1
March 2010
© Becta 2010
http://www.becta.org.uk
NOT PROTECTIVELY MARKED
page 16 of 16

Wired security

Since all network data in a wired network passes over the institution's cables, it is vital that access to network data is by authorised users only, with the correct privileges and rights.

Without the proper security measures in place, users of the network may be able to access information that should be inaccessible to them. Wired network traffic can be intercepted and decoded with commonly available software tools once someone has physical access to the institution's cabling and/or devices (although many switches have protected-port security measures to avoid this problem).

Technical principles		
2.2n	A short, easily understood and realistic ICT Security policy (based on information risk management principles and a framework for risk assessment and policy justification) and Acceptable Use policy *shall* be in place. Both *shall* be applicable to all users of the network.	
2.2o	Unused patch leads *shall* be removed from network equipment.	
2.2p	Routing and switching cabinets *shall* be locked, and all keys strictly controlled.	
2.2q	Cables into institutions or between buildings *should* be located underground or be adequately protected from physical interference.	
2.2r	Network cabling *should* be protected from unauthorised interception or damage by utilising wall cavities and space behind walls wherever possible.	
2.2s	Regular checks *should* be made to ensure that all cables are routed to their correct terminating equipment.	
2.2t	Logical port security *should* be implemented when it is available on the network equipment. When it is not, unused ports on network equipment *should* be disabled.	

Firewalls

It is essential that firewalls are properly installed and configured to protect institutions' systems from unauthorised access.

To ensure that firewalls are installed and configured in a way that does not impede an institution's ability to function efficiently, institutions should liaise with their service provider/s to ensure their needs are met. Where necessary, rules should be applied through cascaded firewalls rather than applied as a blanket across all institutions served by the service provider.

It must be noted that multiple firewalls impede an institution in applying Quality of Service (QoS) across its network and its partner's network, and can prevent applications such as video conferencing from working.

However, where an institution already has an adequate firewall in place and wishes to retain this, it is acceptable for it to do so as long as it liaises with its service provider to ensure that the firewall does not impede the operation of the network and its applications.

Technical principles		
2.2u	Advice on regional firewall policy **shall** be sought from the local authority, Regional Broadband Consortia or other service provider.	
2.2v	Unnecessary network ports **shall** be closed and the default setting **should** be 'deny all'.	
2.2w	Where an institutional firewall is in place, this **shall** be configured so as to be in keeping with LA/RBC firewall policy.	

2.3 Wireless networks

As stated above, wireless networking can provide an additional layer of flexibility to enhance traditional wired networks, allowing access to the network from previously inaccessible locations.

Technical principles		
2.3a	Before a LAN is extended to include wireless LAN (WLAN) technology, a feasibility study and site survey **shall** be undertaken.	
2.3b	Wireless LANs **shall** only be used to supplement and not to replace wired networks.	

Wireless management and security

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

A number of basic security settings are provided by an access point (AP) or the management software of the AP. The basic premise of network security is to only allow authorised users and devices onto the institution's network. Unfortunately, WLANs 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 in an

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk
NOT PROTECTIVELY MARKED

page 18 of 18

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[3]
- interception of wireless signal
- attempted unauthorised network access from inside or outside the institution's buildings

Much WLAN security simply requires some basic 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 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 used by some manufacturers are common across all APs in the manufacturer's range. To enable personalisation and security functions to be managed, an AP is usually supplied with management software that has a combination of the following features:

- Turning off the broadcast of the service set ID (SSID; network name)
- Changing the name of the SSID
- MAC address recognition
- Limiting IP range when the AP acts as a DHCP server
- Setting the maximum number of clients that can associate with an AP
- Ability to manage AP over the WLAN
- 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, it will be able to quickly identify those networks that are unauthorised.

Unauthorised networks can be located by a range of means, including an SSID that is invalid or an AP using a wireless channel that is not self-assigned for the institution's own use. Intruders to a network may also be identified by such things as recognising the reuse of MAC addresses.

---

[3] A rogue AP is 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 malicious reasons.

Technical principles		
2.3c	Wireless management tools *shall* be employed to deploy and maintain WLANs.	🛠
2.3d	Default settings of WLAN equipment *shall* be changed.	🛠
2.3e	WLAN networks *shall* be given a name (an SSID) that cannot be associated with the institution.	🛠
2.3f	SSID broadcasting *should* be disabled by default, and only enabled where there is an identified need.	🛠
2.3g	Regular intrusion-detection checks *should* be undertaken.	📈
2.3h	IP addresses for WLAN clients *should* be limited to the maximum number of devices that could realistically associate with that AP, when DHCP and NAT is performed by the AP.	🛠
2.3i	Features that allow an AP to be administered via the WLAN *should* be disabled.	🛠

2.4 Devices and device management

With a wide range of devices available to, and used in, institutions, it is important that these are managed by the institution to provide security, accessibility and availability every time they are needed.

Technical principles		
2.4a	All network-connected user devices *shall* be equipped with a web browser capable of providing access to the services required by the user of that device.	🛠
2.4b	All network-connected user devices *shall* require authentication from an institution's user before granting access to secured areas of the LAN.	🛠

To protect against viruses and malware, both anti-virus and spyware protection software need to be made available to users.

Version 1
March 2010
© Becta 2010
http://www.becta.org.uk
NOT PROTECTIVELY MARKED
page 20 of 20

Technical principles		
2.4c	All devices subject to known threats, including stand-alone devices and portable ICT equipment, *shall* be protected by an institution approved, recognised anti-virus package. Protection *should* be adaptable to accommodate different or specific rules for different devices	🔧
2.4d	The anti-virus package *shall* provide an automatic update facility for virus definition files.	🔧
2.4e	Anti-virus software *shall* be managed so as to minimise the impact on the day-to-day performance of devices and the network.	📈
2.4f	The software *shall* be set to scan any new media detected or files received or opened by any route.	🔧
2.4g	Anti-virus packages *shall* be kept up to date and all devices *shall* have the most up-to-date virus definitions.	🔧
2.4h	All documents and removable media *shall* be subjected to an anti-virus scan prior to being transferred onto the institution network.	🔧
2.4i	All network users *shall* be educated in safe practice when using any media to transfer data from one system to another, such as memory sticks, etc.	📈
2.4j	All network users *shall* be made aware of their responsibilities for protecting data and keeping it secure.	📈
2.4k	Spyware protection software *shall* be installed on devices where there is a threat from spyware.	🔧
2.4l	All network users *shall* be educated on the dangers and symptoms associated with spyware and viruses.	📈
2.4m	Display technologies *shall* be installed in accordance with PAS 1224	🔧

Remote 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 of data made available for different groups of individuals. For example, educators need to access teaching materials, learners' work areas and administration data from within the institution and external locations. Learners need to access their work areas from outside the institution and will most likely need to have access to relevant institution notices and information. Secure remote access to relevant administration data must be made available away from the institution where necessary and a risk assessment must be carried out before granting such access.

---

[4] http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030154893

Version 1
March 2010
© Becta 2010
http://www.becta.org.uk
NOT PROTECTIVELY MARKED
page 21 of 21

Technical principles		
2.4n	Secure remote access *shall* be provided to selected resources for all educators and to learners as appropriate.	
2.4o	Access to selected data *shall* be offered to parents/carers and school governors.	
2.4p	Remote access solutions *shall* provide a web interface via a standards-based web browser or equivalent for portable devices.	
2.4q	An information risk assessment *shall* be completed before allowing remote access to data. (See also 4.4a)	

On-site access

Many learners and educators have access to their own devices, and it is anticipated that they will wish to use these devices in the institution. Special attention to security measures listed above should be given to ensure protection of the institution's infrastructure.

Technical principles		
2.4r	Infrastructures *shall* offer access to learning and teaching resources via personally owned devices used within the institution.	
2.4s	Infrastructures *shall* offer internet access via locally agreed types of personally owned devices used within the institution.	

3. Connectivity

Broadband connectivity is essential for educational institutions, to support both learning and teaching, and management and administration. Institutions' connectivity requirements are complex: their broadband services must be able to support a wide range of services, content and applications. In addition, broadband usage and the consequential bandwidth and performance required are increasing rapidly across educational institutions.

Broadband services for education should therefore have the following attributes:

- **Performance:** to guarantee delivery of demanding applications and content, such as high-quality video conferencing
- **Capacity:** sufficient capacity to support required applications and services, particularly in relation to concurrent usage (multiple users accessing multiple services simultaneously) and symmetric services (where upload and download bandwidth are equal)
- **Scalability:** capable of growing to meet institutions' developing requirements, particularly in relation to bandwidth
- **Reliability and resilience:** guaranteed availability, with swift remediation in the event of service failures

In the light of these requirements Becta strongly recommends that *schools* employ the broadband services offered by local authorities and/or regional broadband consortia (RBCs) as appropriate. All publicly funded *FE colleges and HE organisations* in the UK are entitled to a Primary Connection to JANET which gives access to a full range of network services and support. Becta strongly recommends that such institutions continue to utilise this.

The aggregated procurement and delivery of services at local, regional and national levels, by local authorities and/or RBCs has led to the successful development of dedicated wide area networks (WANs) serving schools and a range of other educational institutions across the UK. These regional WANs are interconnected via the JANET5 backbone to create the National Education Network[6.]

As of December 2006, all *schools* in England were connected to broadband, meeting the government's target. A number of schools are now connected at speeds which significantly exceed the typical connection bandwidths envisaged at the outset of this programme. For example, in Kent[7], as of December 2008, 50 secondary

---

[5] http://www.ja.net/documents/publications/localauthorities.pdf
[6] http://www.nen.gov.uk
[7] http://www.eiskent.co.uk/UserFiles/File/KCN/KCN-2008-Report-12Jan09.pdf

schools had 100Mbps symmetric connections, and almost 400 primary schools had symmetric 10Mbps connections.

The provision of dedicated infrastructure for education ensures a high-quality service for institutions and users, the performance and capabilities of which could not be replicated via a fragmented, piecemeal approach. It provides a high degree of end-to-end management and control, to ensure infrastructure and services can keep ahead of increasing demands. It also supports the delivery of a range of additional services beyond connectivity, including web and email filtering, access management and simplified sign-on, video conferencing and local and regional content applications, including learning platforms. The aggregated delivery of such services also provides a good fit with the drive from central government to increase efficiency and drive down costs in public sector service delivery. Finally, it greatly reduces the 'heavy lifting' required by individual institutions, ensuring teachers and learners can focus on exploiting rather than procuring and maintaining broadband infrastructure and services.

In summary, some of the key advantages of this approach to connectivity can be expressed as follows:

- Fully managed, regional broadband infrastructure
- Dedicated access links (managed contention)
- A portfolio of services – not just connectivity
- Enables services that could not be delivered as efficiently (or in some cases at all) via a piecemeal approach (access management, video conferencing, high bandwidth 'last mile' links)
- Contractual guarantees and service levels
- Resilient and reliable performance (avoids single point of failure)
- Scalable growth (especially as usage is increases)
- Aggregated service delivery, across both services and sectors (filtering and content, across schools and colleges, libraries and social care)
- Reduced burden on institutions
- Consistency of approach
- Access across the UK to national JANET services and opportunities, such as:
  - internet transit
  - video conferencing
  - authentication and access management.

Although there is no requirement that schools must take the service provided by their local authority or RBC, Becta strongly recommends that schools consider the range of broadband services and safeguards provided by their local authority and/or RBC

very carefully when investigating alternatives, particularly if their LA or RBC's service has been accredited by Becta. Becta strongly recommends that schools consider the many advantages of participation in a collaborative, community-led approach to connectivity, and the significant benefits of being part of a managed, dedicated broadband infrastructure for education, when considering alternative connectivity options

Technical principles	
3a	School broadband connectivity and internet access ***should*** be provided via the relevant local authority and/or Regional Broadband Consortium as a appropriate.

3.1 Core Service Set and underpinning delivery principles

Becta has defined a Core Service Set to exemplify what should be in place as a minimum level of broadband provision for all schools. This describes a baseline set of services that schools' and other educational institutions' broadband connectivity should provide to learners and educators. The Core Service Set is supported by a set of delivery principles that should inform the way these services are provided whilst still affording appropriate regional and local flexibility and choice.

Technical principles	
3.1a	Broadband services ***shall*** provide the Core Service Set as a minimum.
3.1b	Broadband ISP services used ***should*** be Becta accredited.

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk
NOT PROTECTIVELY MARKED

page 25 of 25

The Core Service Set

The Core Service Set comprises three strands: connectivity, applications and safeguards, with each strand being comprised of three component elements:

Connectivity:

- Bandwidth – appropriate to need, scalable and future proof as far as possible, and delivered where it's needed
- Reliability/resiliency/availability – managed, guaranteed ICT services governed by appropriate service levels and contractual arrangements
- Performance – sufficient to provide the required applications (in terms of, for example, response times, latency), including support for demanding applications

Applications:

- Access to internet services
- Communication and collaboration tools – email, video conferencing, VoIP, instant messaging
- Learning resources and tools – content, learning platforms, e-portfolios, MIS, resource discovery and search, online productivity tools

Safeguards:

- Security – of networks and data
- Safety – to guard against inappropriate content and contact (filtering, monitoring, authentication and authorisation)
- Policies and procedures – acceptable use policies, security policies, user education, advice and guidance

Version 1
March 2010
© Becta 2010
http://www.becta.org.uk
page 26 of 26
NOT PROTECTIVELY MARKED

3.2 The delivery principles

Six delivery principles illustrate but do not prescribe the way the Core Service Set should be provided, in recognition of the need to tailor delivery to accommodate local circumstances and requirements.

While different models of delivery will continue to be required to provide broadband services across the country, all models should demonstrate and exemplify:

- Flexibility (especially of location and time, providing appropriate access to other users, for example parents)
- Inclusivity and transparency (pricing, bandwidth, availability, reliability, performance)
- Value for money (supporting delivery efficiencies and economies of scale via aggregating demand, ensuring value for money, reducing the procurement and management burden on institutions)
- Sustainability and scalability (service continuity and service level management, the ability to cope with changing and increasing requirements, reflecting and supporting environmental considerations)
- Quality (ease of use, appropriate and fit-for-purpose services)
- Personalisation – tailored, differentiated services.

It is important that the entitlement is dynamic, developing and capable of changing over time, to prevent the misconception that educational broadband provision is complete and needs no further development or change. Requirements, bandwidths and technologies continue to change and develop at ever increasing rates. The Core Service Set provides a useful framework to structure ongoing regular review and reappraisal of school broadband possibilities and requirements. The newly established Education Network Governing Council is responsible for maintaining and reviewing the core service set and delivery principles[8].

Technical principles	
3.2a	Broadband services *shall* be provided in keeping with the six delivery principles.	⚒

---

[8] [http://partners.becta.org.uk/upload-dir/downloads/page_documents/partners/education_network_governing_council/terms_of_reference_0708.pdf]

4. Learning and management systems

Over the past few years there has been a progressive blurring of the functionality provided by what have traditionally been known as learning platforms and management information systems. As technology evolves and systems become more integrated, it is important to ensure through interoperability that users can integrate high-quality learning tools to meet local needs.

With an increase in interoperability between these systems it is more important for educators, learners, managers and administrators to be able to achieve the functionality they require rather than having set applications imposed on them.

Interoperability is the key factor when looking at the functionality that different products offer, as unless they are starting from scratch, institutions are likely to already have tools and systems that provide some of the required functions and it is important that any new tools and systems can share information effectively with existing ones. It is equally important that institutions have free choice of which tools and systems they wish to use and are not 'locked in' to a single provider.

As stated in Core Principles, suppliers of learning and management services **shall** adopt open standards to ensure their products and services will meet the needs of the institution.

	Technical principles	
4a	New systems **shall** be able to interoperate openly with other (existing) systems using open standards.	📈
4b	Systems **shall** comply with best practice guidance for data handling security.[9]	📈
4c	Access to online resources via the UK Access Management Federation for Education and Research **shall** be provided.	⚒
4d	Development of, and changes to, learning and management systems **shall** be based on needs assessments derived from appropriate Becta tools such as the Information Management Strategy Framework, the Self-Review Framework or Generator.	📈
4e	Development of, and changes to, learning and management systems **shall** follow a planned implementation strategy that ensures staff and student consultation where appropriate.	📈

---

[9]See http://www.becta.org.uk/schools/datasecurity and
http://www.becta.org.uk/feandskills/datasecurity

4.1 Learning tools and services

A key use of technology in learning and teaching centres around the creation, location and use of digital learning resources, by both learners and teaching staff. Resources range from simple assets without context to complex leaning objects with structured and sequenced learning objectives, and aggregations of such learning objects.

Many communication and collaboration activities now also generate content or resources that could be used as evidence in an assessment, or as the focus of learning and teaching activity, and the management and interoperability of these assets is becoming increasingly important.

To access and manipulate these resources, an institution should offer a learning platform to its users. The learning platform could be a comprehensive commercial offering, or an aggregation of disparate tools including free Open Source tools. It is unlikely that any one solution will meet all user needs, and flexibility and personal preference in tools is important. Innovation with new tools and techniques should be supported in order to provide as rich and coherent a learning environment as possible. The use of open standards helps ensure interoperability.

Technical principles		
4.1a	System interactions and data *shall* be in open interoperable formats that support creation, editing and repurposing for a range of purposes including teaching and learning, presentation, communication, assessment and reflection, all of which could be done independently or in collaboration, synchronously and asynchronously.	🛠
4.1b	Any system or set of applications or services *shall* associate information with a resource and support the classification of resources through the use of tags, by adding, editing or removing metadata manually and automatically including information such as peer review and comment.	🛠
4.1c	The system *shall* support the safe and secure management of resources, including the capacity to delete and archive items.	🛠
4.1d	The system *shall* support the import and export of resources, tags and data, manage playlists and bookmarks in a way that supports learners as they move between educational settings and phases.	🛠
4.1e	The system *shall* support a range of user permissions (that is, grant and restrict access) to resources, including portfolios, lesson plans, schemes of work and course materials with a range of user types, including learners, teaching staff and others. The access to the resources *shall* be controllable through schedules, timetables, rights and permissions, user profiles, usage data and time constraints.	🛠
4.1f	The system *shall* support the access to resources or collections of resources by groups or individuals either publicly or securely, allowing	🛠

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk
NOT PROTECTIVELY MARKED

page 29 of 29

	others to provide feedback and comments privately or collaboratively. This would include the submission of usage data.	
4.1g	The system *shall* be able to support the preview, load and launch of resources. The system *shall* permit interaction, independently or collaboratively, with resources including digital assets, presentations, assessment items, packaged resources etc. The user interaction *shall* generate usage data which *shall* be stored for tracking and reporting.	⚒
4.1h	The system *shall* support the capacity to browse and/or search locally and globally for resources and filter results according to parameters such as file type, licence, curriculum mapping etc. making use of stored metadata and indices. Information about resources *shall* be displayed to the user to facilitate effective selection. The search mechanism *shall* be able to retrieve and/or receive metadata and information from multiple sources such as user generated information tags, resource lists and playlists. The search mechanism *shall* be able to search multiple sources in a federated manner. When considering searching for digital learning resources, the solution *should* be consistent with the national Content Ecosystem Strategy.	⚒
4.1i	The system *shall* provide access to reports based on resource usage data. Reports *shall* provide users with information on progress and achievement and allow analysis of individual and group statistics and access to feedback and peer review.	⚒
4.1j	Where external services are used to provide additional functionality, they *shall* provide open Application Programme Interfaces (APIs) to facilitate interoperability.	⚒

4.2 Data interoperability

The provision of interoperability standards and governance arrangements for school, college and local authority systems enables diverse applications within the education, skills and children's services sector to interact and share data efficiently, reliably and securely, regardless of the platform hosting the applications.

Becta estimates that with the adoption of the Systems Interoperability Framework across the core services required within institutions it is possible that by 2014, data for 80 per cent of pupils will be 'recorded once and used many times' within integrated data systems, an increase of possibly 40 per cent over this period. This will support both administrative efficiencies and enable more effective real-time information handling and reporting.

Based on implementation in the US and the UK proof of concept, a conservative estimate of administrative time saved is 1.6 hours per pupil per year. For the additional 2.9m pupils (40 per cent), this is equivalent to nearly 3000 administrative FTEs, or approximately £71m annually.

Technical principles		
4.2a	Systems **shall** share information in an open, secure manner, such as via the Systems Interoperability Framework.	
4.2b	Access to a Zone Integration Server **shall** be provided to enable use of Systems Interoperability Framework if required.	
4.2c	In the school sector, Zone Integration Servers **should** be provided by the local authority or regional broadband consortia.	

4.3 Simplified sign-on

With an increase in the amount of online resources available to learners, teachers and staff, there is a need for simplified sign-on (SSO) to prevent users having to manage multiple usernames and passwords. Implementing SSO in such a way that a user will need only to enter an institutional ID and password will remove the complexity of having to manage multiple IDs, passwords and authentication challenges. The user can also be assured that personal information is not being disclosed unnecessarily to third parties. Users will have the ability to access resources outside the school environment, such as at home or in a public library, subject to the validity of licences. Managed attributes will allow appropriate content to be presented with minimal end-user intervention.

Technical principles		
4.3a	Simplified sign-on via the UK Access Management Federation **shall** be implemented. For accessibility, sign-on must not be a barrier and **should** include sign-on other than via username and password, and be no more than the appropriate user access security required for a resource.	
4.3b	For **Schools** the provision of simplified sign-on **shall** be aggregated at a level above the institution, typically via a local authority or regional broadband consortia identity provider (IdP).	
4.3c	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 lower case and capital letters; Passwords **should** be changed frequently.	
4.3d	Shared (as opposed to personal) user IDs **should** only be used for the youngest of learners.	
4.3e	Shared passwords **should** be avoided but where shared passwords are deemed essential/appropriate, limited access privileges **should** be used.	
4.3f	Passwords **shall** be changed when compromise is suspected or feared.	

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk

NOT PROTECTIVELY MARKED

page 31 of 31

4.4 Information security

The Data Protection Act 1998 requires all organisations to secure any personal data they hold – this covers data held both electronically and on paper. The security of this information is the responsibility of everyone in the institution and needs to be embedded into culture and ways of working within and across the institution.

Technical principles		
4.4a	Network infrastructure and services *shall* conform to Becta's data handling security guidance.[10]	

---

[10] http://www.becta.org.uk/schools/datasecurity and http://www.becta.org.uk/feandskills/datasecurity

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk
NOT PROTECTIVELY MARKED

page 32 of 32

5. Environmental sustainability

There is an environmental impact to consider when using and choosing ICT in institutions. However, careful use of technology can reduce energy costs and the need for travel, and help reduce the environmental impact of paper consumption and waste of other consumables.

5.1 Power management

Much of a school's ICT carbon output can be reduced by adopting new behavioural practices. However, the technology itself can work against this – for example, screensavers do not save energy and some use significantly more, particularly if they prevent the machine from going into standby or hibernate mode.

Power management technology can support users in saving energy. The universal deployment of power management offers the opportunity for technology enabling itself to automatically put itself into lower power modes, such as when inactive, without requiring active human intervention (but allowing user over-ride where necessary).

Centralised power management

Stricter adherence to policies can be enforced by appropriate use of enterprise/network management or similar software packages which provide or facilitate centralised control of power-saving settings. Institutions can decide and record policy guidelines for system updates, for example allowing devices to be left on at certain times if 'Wake-on-LAN' is implemented.

Technical principles		
5.1a	Power management capability ***shall*** be present and enabled on all devices.	🛠
5.1b	Power management capability ***should*** include centralised technical solutions such as 'Wake-on-LAN'.	🛠
5.1c	All active screensavers ***shall*** be disabled.	🛠
5.1d	Software agents that prevent systems from going into power-saving modes ***should*** be disabled.	🛠
5.1e	Whenever possible, each device ***should*** be labelled with specific instructions on saving power.	🛠
5.1f	Non-networked technology ***should*** have timer-switches applied.	🛠

5.2 Energy efficiency and consolidation

It is important to consider energy efficiency and lower power alternatives when selecting or replacing equipment and devices, such as in the form of multi-functional device alternatives and centralisation of processing power. Newer technology can

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk
NOT PROTECTIVELY MARKED

page 33 of 33

use significantly less energy than older technology, whether it is in the power supply, the processor or the display technology.

Technical principles		
5.2a	Devices *shall* meet the current best requirements in energy performance (e.g. Energy Star 5).	🛠
5.2b	Devices *should* meet the performance requirements of Energy Saving Recommended.	🛠
5.2c	Policies *shall* be in place to review and optimise utilisation.	📈
5.2d	Where large numbers of servers are in commission, server virtualisation *shall* be used to consolidate utilisation of servers, where this will lead to direct operational energy savings, or significant reductions in embedded carbon of new equipment and where the surplus servers can be reused.	🛠

5.3 Positioning, cooling and use of waste heat

Careful preparatory work when designing or choosing equipment, rooms and installations can save a significant amount of energy.

Heat and cooling
Reduce cooling and make use of 'free-cooling' as much as possible. Best practice is not to cool server rooms below the advised operating temperatures stated by the manufacturer.

Technical principles		
5.3a	Equipment *should* be positioned with care to maximise energy conservation.	🛠
5.3b	Devices *shall* meet current good practice in calculating greenhouse gas emissions.	📈

5.4 Consumables and sustainable use

Devices such as printers, photocopiers and faxes consume energy, ink and paper. However, there are a variety of techniques for reducing this consumption.

Version 1
March 2010
© Becta 2010
http://www.becta.org.uk
NOT PROTECTIVELY MARKED
page 34 of 34

Lifecycle extension

Consider replacing parts, retrofitting newer modules or refurbishing equipment.

Technical principles		
5.4a	Print management capability **shall** be present.	⚒
5.4b	Print management packages and other software **should** be used to reduce use of consumables and energy. Used ink cartridges **should** be recycled.	⚒
5.4c	Policies **should** be in place to optimise use of duplex and grey-scale printing.	📈
5.4d	Green ICT best practices **should** be embedded and these **should** include environmental impact assessments. Policies **should** be in place to extend the lifecycle of all ICT equipment where this will reduce the environmental impact. Whenever possible, each device **should** be labelled with specific advice on sustainable use.	📈
5.4e	Systems **should** be designed for upgrading using commonly available tools as well as being designed for product lifetime extension, disassembly, reuse and recycling.	📈

5.5 Reducing energy consumption across the institution

When creating an energy policy, energy meter readings can give a baseline assessment and be helpful in creating, raising and maintaining awareness of environmental impact. However, there are systems that can track electricity consumption of network-connected devices

Control systems

By incorporating an ICT plan into an institution-wide approach to carbon reduction, institutions can take every opportunity to use technology to reduce the need for energy consumption.

Technical principles		
5.5a	The energy consumption of the ICT Services **shall** be measured, monitored and reported upon.	📈
5.5b	Whenever possible, equipment **should** have functionality to report its energy use or hours of use and for network-connected devices this **should** be to central systems.	⚒
5.5c	Whenever possible, full use **should** be made of the existing ICT to support and control building management systems in conserving energy and reducing waste.	⚒

Version 1
March 2010
© Becta 2010

http://www.becta.org.uk
NOT PROTECTIVELY MARKED

page 35 of 35