Bolton Schools ICT

Putting Schools First

TECHNOLOGY STANDARDS FOR PRIMARY SCHOOLS 2023

CONTENTS

DFE Standards

Timetable for meeting Technology Standards

Technology Standard	NOW	ASAP	AT NEXT UPDATE
Broadband Internet Standards			
Schools and colleges should use a full fibre connection for their broadband service			✓
Schools and colleges should have a backup broadband connection to ensure resilience and maintain continuity of service			✓
Schools and colleges should have appropriate IT security and safeguarding systems in place, under both child and data protection legislation	✓		
Network Switching Standards			
The network switches should provide fast, reliable and secure connections to all users both wired and wireless			✓
Have a platform that can centrally manage the network switching infrastructure			✓
The network switches should have security features to protect users and data from unauthorised access			✓
Core network switches should be connected to at least one UPS to reduce the impact of outages			✓
Network Cabling Standards			
Copper cabling should be Category 6A (Cat 6A)			✓
Optical fibre cabling should be a minimum 16 core multi-mode OM4			✓
New cabling should be installed and tested in line with the manufacturer's guidance, warranty terms, and conditions			✓
Wireless Network Standards			
Use the latest wireless network standard approved by the Wi-Fi Alliance			✓
Have a fully functional signal from your wireless network throughout the school or college buildings and externally where required			✓
Have a solution that can centrally manage the wireless network			✓
Install security features to stop unauthorised access			✓
Cyber Security Standards			
Protect all devices on every network with a properly configured boundary or software firewall	✓		
Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date	✓		
Accounts should only have the access they require to perform their role and should be authenticated to access data and services		✓	
You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication		✓	
You should use anti-malware software to protect all devices in the network, including cloud-based networks		✓	
An administrator should check the security of all applications downloaded onto a network		✓	
All online devices and software must be licensed for use and should be patched with the latest security updates		✓	
You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site		✓	
Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack		✓	
Serious cyber-attacks should be reported		✓	
You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation	✓		

Train all staff with access to school IT networks in the basics of cyber security		✓ Within 12 months	
Filtering and Monitoring Standards			
You should identify and assign roles and responsibilities to manage your filtering and monitoring systems	✓		
You should review your filtering and monitoring provision at least annually	✓		
Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning	✓		
You should have effective monitoring strategies that meet the safeguarding needs of your school or college	✓		
Cloud Solution Standards			
Use cloud solutions as an alternative to locally-hosted systems, including servers		✓	
Cloud solutions must follow data protection legislation	✓		
Cloud solutions should use ID and access management tools		✓	
Cloud solutions should work on a range of devices and be available when needed	✓		
Make sure that appropriate data backup provision is in place	✓		
Servers and Storage Standards			
All servers and related storage platforms should continue to work if any single component or service fails	✓		
Servers and related storage platforms must be secure and follow data protection legislation	✓		
All servers and related storage platforms should be energy-efficient and set up to reduce power consumption, while still meeting user needs	✓		
All server and related storage platforms should be kept and used in an appropriate physical environment	✓		

This document focuses on the guidance published by DFE on meeting digital and technology standards in school and colleagues found at: Government technology standards and guidance - GOV.UK (www.gov.uk) This summary is designed for school leaders to introduce the concept of what, at a high level, is required to take place. The document then goes on to the technical details, referencing the DFE technical standard document where they exist and providing additional detail when they do not so that a holistic solution is referenced.

Broadband Internet Standards

The Bolton Schools ICT broadband SLA provided connection exceeds the speed required in this standard.

The connection is protected by a Sophos Unified Threat Management device configured at the 'edge' of the network. This is maintained and monitored by SICT. This provides Firewall and Web Filtering. From September 2023 the monitoring is provided by a product called FastVue which works alongside the web filter to provide reports and alerts.

BSICT are currently undergoing a review of this service, and whilst it is likely the product may change, this will be at least an equal match to the current solution in place, with some improvements due to advances in technology and services offered by supplies. For example, a backup connection will be provided in the next round of updates to the broadband connections in schools.

Network Switching Standards

All the switches currently available and those supplied in the last 5 years from Bolton Schools ICT meet the following requirements:

1. To provide 1Gbps connectivity to end user devices.
2. Centrally managed and monitored.

Our default switch configuration securely separates the network into 3 parts, internal secure network, external network, guest wireless network, and VOIP Telephony networks. Using VLANs prevents these separate networks from accessing each other.

Bolton Schools ICT can quote for new switches which meet the requirement for higher speeds to servers and infrastructure devices on request.

It is important to note that the ability of the switch to deliver this higher speed is dependent on the specification and quality of physical cabling, and this may also need to be upgraded to meet the separate DfE cabling standard when new networking equipment is installed.

A UPS can be provided to provide power backup to your core switches as necessary, this is often of limited benefit to primary schools.

Bolton Schools ICT can survey and audit your network switches and provide recommendations to help you meet standards if not already. This can present a significant cost to school to meet, so a cost-benefit analysis would need to be carried out which we can advise on potential benefits.

Switch: Meeting digital and technology standards in schools and colleges - Network switching standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Network Cabling Standards

Having your school fully rewired with new cabling is a major expense.
Most schools will have Category 5E or 6 cabling. This is suitable to provide 1Gbps connectivity to the desktop as required in the switching standards.
Category 6A cabling is capable of supporting 10Gbps which is generally only used for infrastructure links.

In order to meet the network cabling standards, it is highly likely that you will need to upgrade all your network cabling. Only new build schools or those with recently installed cabling are likely to meet this standard.
Bolton Schools ICT can carry out an initial basic survey to advise and assist with a cost-benefit analysis, but for a full quote or for work to be carried out you will need to engage with a cabling contractor. Bolton Schools ICT can assist you with providing the specification to the contractor and engaging in technical discussions.

Cabling: Meeting digital and technology standards in schools and colleges - Network cabling standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Wireless Network Standards

The newest wireless access points available from Bolton Schools ICT meet the technical requirements of this standard. Bolton Schools ICT offer a wireless survey as part of quoting for the network and can arrange coverage across school as necessary.
New installs will all have a segregated guest wireless network as standard, and older installs are being upgraded on a rolling basis where possible.

Schools are not required to meet this standard until your existing setup is replaced when it is either underperforming or unsupported. However, you will likely need to consider upgrading your network cabling as well at the same time, as installing a new wireless network triggers the requirement to meet the network cabling standards which present a considerable expense to school.

Cyber Security Standards

All schools utilising Bolton Schools ICT Broadband SLA are provided with an industry leading edge firewall and filtering device. They also get Sophos anti-virus as part of this SLA. This meets all the relevant requirements and is monitored and maintained as part of the SLA agreement.

Bolton Schools ICT will maintain network accounts based on requests from school and will keep a log of requests via our calls system. It is the responsibility of each school to ensure that they keep these accounts up to date and

request account deactivation when staff leave. Bolton SICT can advise on how to maintain the security of your network drives so that data can only be accessed by those with permission.

Bolton Schools ICT recommend that schools use the "Cyber Security Training for School Staff" materials from the NCSC. Schools must ensure that they deliver this training every year. It is recommended that a log is kept of this training and staff completing the training download their certificate. This training should also be offered to school governors with the expectation that at least one governor completes the training every year. Any new members of staff must complete this Cyber security training as part of their induction into the school.

As part of our service into schools, Bolton Schools ICT will review the suitability, quality and effectiveness of these measures every year.

Filtering and Monitoring Standards

Schools utilising the Bolton Schools ICT broadband SLA meet this standard. Over the summer we have purchased and deployed a new monitoring system to meet the requirements for monitoring and alerts. Our existing web filter meets the filtering requirements.

Cloud Solution Standards

Schools ICT manage a Bolton-wide tenancy on Microsoft 365 for all schools utilising this service. This includes email, Teams and some schools use OneDrive/SharePoint as well. This is a hybrid solution, as schools also have a local server.

Data in our Microsoft 365 tenancy is stored within the UK or EU.

The cloud data transfer is protected behind HTTPS encryption. Logon requires multi-factor authentication when accessed outside the school secure network.

There is currently no additional backup in Microsoft 365 beyond that provided by Microsoft where deleted items can be recovered within around 30 days. Data which needs to be properly backed up must be kept on the school server.

We are investigating options for schools who wish to move more of their services into the cloud and will provide information in due course, or if you would like more information, please contact us.

Servers and Storage Standards

As part of the SLA, SICT will monitor your server for failure using Dell's OpenManage software, and Microsoft Systems Centre Operations Manager. If a failure is detected a technician will investigate and a quote will be sent to schools for replacement hardware if not covered by warranty.

All new servers provided after September 2023 will come with multiple power supplies for redundancy, this will present an increased cost.

All servers provided by Bolton Schools ICT come with 3 year's onsite warranty and maintenance from date of installation.

Bolton Schools ICT will keep your servers up to date and patched.

Your server should be kept in a secure location in school that is not accessible to unauthorised persons. This can either be a locked cupboard, or a secure purpose-built room. SICT can assist with moving your server if this is necessary to meet this requirement. You may need to have extra power and data points fitted, and the room or cupboard must not be used for other purposes.