

TITLE OF POLICY:	SCHOOL TECHNICAL SECURITY POLICY (including filtering and passwords)
PREPARED BY:	BEN TIPTON
DATE POLICY PRESENTED TO GOVERNORS:	AUTUMN 2024
DATE DUE FOR REVIEW:	AUTUMN 2026

SCHOOL TECHNICAL SECURITY POLICY

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

The management of technical security will be the responsibility of Bolton ICT support team.

Technical Security

Policy statements

The school and Bolton ICT support team who the school employs will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

There will be regular reviews and audits of the safety and security of school technical systems

Servers, wireless systems and cabling must be securely located and physical access restricted

Appropriate security measures are in place, such as school filtering and internet security such as Sophos, to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff within Bolton ICT who manage technical issues.

All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the Online Committee (or other group).

Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Computing coordinators are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

Mobile device security and management procedures are in place

School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

Remote management tools are used by staff to control workstations and view users activity

An appropriate system is in place through the ICT fault log for users to report any actual potential technical incident to the Online Coordinator / Network Manager / Technician (or other relevant person, as agreed).

An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.

An agreed policy is in place within the AUP regarding the downloading of executable files and the installation of programmes on school devices by users

An agreed policy is in place within the AUP regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

An agreed policy is in place within the AUP regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.

The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc..

Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Committee (or other group).

All school networks and systems will be protected by secure passwords that are regularly changed

The administrator passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe.

Passwords for new users, and replacement passwords for existing users will be allocated by Bolton ICT technical support team. Any changes carried out must be notified to the manager of the password security policy (above).

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below

requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil / student)

Staff Passwords

All staff users will be provided with a username and password by Bolton ICT support team who will keep an up to date record of users and their usernames.

the password should be a minimum of 8 characters long and must include three of 8 uppercase character, lowercase character, number, special characters

must not include proper names or any other personal information about the user that might be known by others

the account should be “locked out” following six successive incorrect log-on attempts

temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on

passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)

passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school

should be changed regularly throughout the year – once every 3-6 months.

should not re-used for 6 months and be significantly different from previous p the last four passwords cannot be re-used

should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
should be different for systems used inside and outside of school

Student / pupil passwords

All users will be provided with a username and password by the computing coordinator who will keep an up to date record of users and their usernames.

Students / pupils will be taught the importance of password security

The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in lessons through e-safety lessons and through specific events such as internet safety day.
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

Bolton ICT support team and or the computing coordinator will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the headteacher and the computing coordinators in conjunction with Bolton ICT support team that provide the filtering system. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to a second responsible person (Computing coordinator or headteacher):

All users have a responsibility to report immediately to the computing coordinator or headteacher any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

Either - The school maintains and supports the managed filtering service provided by Bolton ICT support team
The school has provided enhanced / differentiated user-level filtering through the use of Bolton ICT filtering programme.

In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).

Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.

Any filtering issues should be reported immediately to the filtering provider.

Requests from staff for sites to be removed from the filtered list will be considered by the technical staff and computing coordinators. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Group.

Education / Training / Awareness

Pupils / students will be made aware of the importance of filtering systems through the online education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

the Acceptable Use Agreement
induction training
staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the computing coordinator who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

the second responsible person – Headteacher or computing coordinator
Online Group
External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.