Pendle
Education Trust

shine
Castercliff Primary Academy

Technical Security Policy 2022-2023

Author of Policy:	Kirsty Johnson
Policy Approved By:	Mark Sherwin
Date:	November 2022
Review date:	November 2023

Technical Security Policy
(including filtering and passwords)

Key Providers

Broadband: BT Lancashire
Filtering: Lightspeed Systems (provided by BT Lancashire)
Filtering and Monitoring: Impero
Anti-virus protection: Sophos (provided by BT Lancashire)

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 academy will be responsible for ensuring that the academy 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 data protection 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 the academy technical systems.
- There is oversight from senior leaders and the Online Safety Group as appropriate and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the Pendle Education Trust IT Support team and the Online Safety Leader.

Technical Security

Policy statements

- There will be regular reviews and audits of the safety and security of the academy's technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, 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 – Pendle Education Trust IT Support team and the Online Safety Leader.
- All users will have clearly defined access rights to academy technical systems. Details of the access rights available to groups of users will be recorded by the Pendle Education Trust IT Support team and will be reviewed, at least annually, by the Online Safety 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. *(See Password section below).*
- The Pendle Education Trust IT support team 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. (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.)
- Mobile device security and management procedures are in place, as outlined in the Online Safety policy and in the relevant Acceptable Use Policies *(Appendices 3 & 4 of the Online Safety Policy)*.
- Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the relevant Acceptable Use Policy *(Appendices 3 & 4 of the Online Safety Policy)*.
- Remote management tools (AB Tutor) are used by staff to control workstations and view users activity.
- Users must report any actual / potential technical incident / security breach to the Online Safety Leader and/or recorded on CPOMS (if the incident directly involves a pupil).

- An agreed Acceptable Use Policy is in place (*Appendix 4 of the Online Safety Policy)* for the provision of temporary access of "visitors" (e.g. trainee teachers, supply teachers, visitors) onto the school system; this includes the use of a 'visitor' login with restrictions on access to the school network.
- An agreed Acceptable Use Policy is in place *(Appendices 3 & 4 of the Online Safety Policy)* regarding the downloading of executable files and the installation of programmes on school devices by users.
- An agreed Acceptable Use Policy is in place (*Appendices 3 & 4 of the Online Safety Policy)* regarding the extent of personal use that users (staff / students / pupils / community users) are allowed on school devices that may be used out of school, school devices must not be used by family members in any circumstances.
- An agreed Acceptable Use Policy is in place (*Appendices 3 & 4 of the Online Safety Policy)* 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 virus software against malicious threats from viruses, worms, trojans etc.
- Personal data must not 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, but not limited to, networks, devices and e-mail.

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 Pendle Education Trust IT Support team and will be reviewed annually by the Online Safety Group.
- All school / academy networks and systems will be protected by secure passwords. The "master / administrator" passwords for the academy systems, used by the Pendle Education Trust IT Support team must also be available to the Principal and Online Safety Leader, with copies kept securely in school. Two factor authentication may also be required for these accounts.
- All users 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.

- Passwords for new users, and replacement passwords for existing users will be allocated by the Pendle Education Trust IT Support team.
- Where passwords are set / changed manually, requests for password changes should be authenticated by the Online Safety Leader to ensure that the new password can only be passed to the genuine user.
- Passwords for web-based services (e.g. CPOMS) where sensitive data is in use may require two factor authentication. Where the two factor authentication requires a physical item (e.g. Merilock key used for CPOMS), this must be stored separately from the laptop when in transit – to avoid both being lost / stolen together. Where a 'Soft Key' (e.g. use of a mobile app) is used, this must be on a device that is secured with a password or passcode.

Staff Passwords

- All staff users will be provided with a username and password by the Pendle Education Trust IT 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 – uppercase character, lowercase character, number, special characters.
- The account will 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, will be enforced to change immediately upon the next account log-on.
- Passwords will not be displayed on screen and will 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.
- There is no requirement for regular password changes for school systems, in line with advice from the National Cyber Security Centre (GCHQ): *"Regular password changing harms rather than improves security, so avoid placing this burden on users. However, users must change their passwords on indication or suspicion of compromise."* https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Pupil Passwords

Pupil users in KS1 will have Year group logons, with age-appropriate passwords. Pupil users in KS2 will have individual logons with individual passwords. These logons provide limited access to the school network. Pupils will be taught the importance of password security as a routine part of ongoing Online Safety education and via the #BESAFE rules.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users through ongoing Online Safety education.

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

- at induction
- through this Technical Security policy
- through the Staff Acceptable Use Policy (*Appendix 3 of the Online Safety 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 safety 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.

Castercliff Primary Academy has considered carefully and decided the following:

- To allow flexibility for sites to be added or removed from the filtering list.
- Responsibility for decisions, checks and balances regarding which sites are to be added or removed from the filtering list will be that of the Online Safety Leader and Academy Principal.
- In addition to filtering, pupils will not access the internet when unsupervised under any circumstances. Monitoring of pupil's activity when using computers will also be monitored in lessons using Impero.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Pendle Education Trust IT Support team and the academy's Online Safety Leader. 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:

- Approved by at least two members of the Online Safety Group prior to changes being made.
- Logged via the PET IT Support helpdesk (support@pendleeducationtrust.co.uk).
- Reported to the Online Safety Group in the form of an audit of the change control logs.

All users have a responsibility to report immediately to the Online Safety Leader 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 the 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.

- The academy maintains and supports the managed filtering service provided by Lightspeed Systems via BT Lancashire Services.
- The school has provided enhanced / differentiated user-level filtering through the use of Lightspeed Systems.
- Mobile devices that access the academy internet connection (whether academy 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 at least two members of the Online Safety Group. If the request

is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through ongoing online safety education. 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 Staff Acceptable Use Policy (*Appendix 3 of the Online Safety Policy)*
- induction training
- staff meetings, briefings, ongoing CPD.

Parents will be informed of the school's filtering policy through Online Safety awareness sessions, information provided on the school website and academy newsletters.

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

- Staff users may request a change to the filtering system; requests must have a strong educational basis. Requests from staff users must be made to the Online safety Leader directly. The Online Safety Leader will review the request and consult a second member of the Online Safety Group or the Academy Principal and then decide if the request should be forwarded to the Pendle Education Trust IT Support team to change the filtering.
- Requests to Pendle Education Trust IT Support team will be made by the Online Safety Leader via the IT Support helpdesk system to ensure a log of approved requests is kept.
- A retrospective review of approved requests for filtering changes will be undertaken at the regular Online Safety Group meetings.

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 Online Safety Leader 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 in this Technical Security Policy, the Online Safety Policy and the relevant Acceptable Use Policies. Monitoring will take place as follows: pupil users must not access the Internet / use online tools without adult supervision. AB Tutor may also be used to monitor use of computers in school.

Audit / Reporting

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

- The Academy Principal
- Online Safety 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. The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary.

Pendle
Education Trust

Pendle Education Trust
Nelson and Colne College, Scotland Road, Nelson, BB9 7YT
Tel 01282 440 249 Email contact@pendleeducationtrust.co.uk
Company Registration Number: 08263591
Place of Registration: England and Wales