Pendle
Education Trust

Technical Security Policy
(including filtering and passwords)

Author of Policy	Catherine Jermyn, DSL Pendle Primary Academy & Rob Weidner, ITL Team Leader
Policy Approved by	Online Safety Group
Date	November 2022
Review Date	November 2025

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

Technical Security Policy (including filtering and passwords)

This policy covers all Pendle Education Trust (PET) schools. This policy and its effectiveness is monitored on a termly basis by the Online Safety Group; in light of any significant new developments in the use of digital technologies, new threats to online safety or incidents that have taken place, this policy may be reviewed at any time.

Key Providers in all settings

Broadband: LEDS (Lancashire Educational Digital Services)

Filtering: NetSweeper (provided by LEDS)

Filtering and Monitoring: Impero

Anti-virus protection: Sophos (provided by LEDS)

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 Pendle Education Trust Information Technology for Learning team (PET ITL team) alongside each school's Online Safety Leader (this is the DSL unless the school has a named Online Safety Leader in their school Online Safety policy) and school technical staff, 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 PET GDPR 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 systems.
- There is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the PET ITL team.

Technical Security Policy Statements

The school, working together with the PET ITL team, will be responsible for ensuring that their 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 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 the technical requirements outlined by the DfE Meeting digital and technology standards in schools and colleges https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges;

- 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 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;

- 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 PET ITL team and will be reviewed, at least annually;

- 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;

- the PET ITL team is 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 and outlined in the Online Safety policy and Acceptable Use of ITL systems and resources policy;

- the Trust ITL team and each school's technical staff, including the Online Safety Leader, 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 agreement;

- remote management tools are available to staff to control workstations and view user activity;

- an appropriate system is in place via email to the IT Helpdesk for staff users to report any actual/potential technical incident to the PET ITL team. Staff users are able to report directly to the Helpdesk via email but may report first to their school's Online Safety Leader. Pupil users report technical incidents first to a member of staff to pass on to the IT Helpdesk via email.

- an agreed policy is in place, using the visitor login, for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school's systems and is subject the signing of the Visitor IT Acceptable Agreement;

- an agreed policy is in place as outlined in the Staff IT Acceptable Use Agreement regarding the downloading of executable files and the installation of programmes on school devices by users;

- an agreed policy is in place as outlined in the Staff IT Acceptable Use Agreement for staff users and in the Child-Parent IT Equipment Loan Agreement for pupil users regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school;

- an agreed policy is in place as outlined in the Online Safety policy and Acceptable use of ITL systems and resources policy regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices;

- each school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.;

- personal data must be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

These statements apply to all users.

- All school networks and systems are protected by passwords.

- All users have clearly defined access rights to school technical systems and devices.

- All users (adults and pupils) have responsibility for the security of their usernames and passwords and must not share them or 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.

- All users will be provided with a username and password by the PET ITL Team or a member of school technical staff, who will keep an up-to-date record of users and their usernames.

Password requirements

- Passwords should be a minimum of 12 characters in length and be easy to remember, but difficult to guess or crack.

- 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.

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

- Passwords must be changed on first login to the system.

Pupil passwords

- Passwords for pupils in KS3 & KS4 should be a minimum of 12 characters in length.

- Passwords for pupils in KS2 will be set in the form of a 4-digit numerical pin number.

- Where devices in EYFS, KS1 or KS2 are shared (e.g. used on a 1:2 basis), classroom staff may choose to use a 'whole class login', with an age-appropriate password. This login provides limited access to the school network and must only be used with close adult supervision and where static IP addresses are in place to ensure that filtering and monitoring logs can be matched back to a specific device. Classroom staff must keep a record of which child uses which device to ensure that any individual who may have infringed the rules set out in the policy or the acceptable use agreement / charter / #BESAFE rules can be identified.

- If records of pupil usernames and passwords are kept in paper-based form, they must be kept securely by the class teacher when not required by the user.

- Pupils will be required to change their password if it is compromised.

- Pupils will be taught the importance of password security as part of the school's online safety curriculum, this should include how passwords are compromised, and why these password rules are important.

Technical staff / administrators

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level with two factor authentication for such accounts, where possible.

- An administrator account password for the school's systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access.

- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.

- It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.

- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by the PET ITL Team or school technical staff. This password should be temporary and the user should be forced to change their password on first login.

- Requests for password changes should be authenticated by the PET ITL Team or school technical staff to ensure that the new password can only be passed to the genuine user.

- Suitable arrangements should be in place to provide visitors with appropriate access to systems.

- In good practice, the account is "locked out" following five successive incorrect log-on attempts.

- Passwords should not be displayed on screen, and is securely hashed when stored (use of one-way encryption).

Password policy – staff awareness

Staff users will be made aware of the password policy through:

- Induction

- This technical security policy

- through the PET Staff IT Acceptable Use Agreement

Password policy – pupil awareness

Pupil users will be made aware of the password policy through:

- The online safety curriculum
- Through the #BESAFE rules / pupil acceptable use agreements / school charters

Password monitoring

The PET ITL Team will ensure that records are kept of:

- User IDs and requests for password changes
- User logons
- Security incidents related to this policy

Filtering

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.

Responsibilities

The responsibility for the management of each school's filtering policy will be held by the PET ITL team and 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 recorded via PET Helpdesk e-mail request.
- be reported to the termly Online Safety Group meeting.

All users have a responsibility to report immediately to their school's Online Safety Leader and/or PET ITL Team 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 pupils and customised filtering changes are managed by the school. Illegal content is filtered by the 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.

- The school maintains and supports the managed filtering service provided by LEDS.
- The school has enhanced/differentiated user-level filtering through the use of the Netsweeper 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 Online Safety Leader or SLT.
- Mobile devices that access the school's 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 PET ITL Team and/or members of school technical staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Pupils will be made aware of the importance of filtering systems through the online safety curriculum. 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:

- PET Staff IT Acceptable Use Agreement
- Induction training
- Staff meetings / briefings / updates

Parents will be informed of the school's filtering policy through the relevant parental consent / acceptable use agreement / charters and through online safety awareness sessions, newsletters etc.

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 safety policy and the acceptable use agreement. Monitoring will take place as follows: in EYFS, KS1 and KS2 pupil users must not access the internet / use online tools without adult supervision. Impero may also be used to monitor the use of devices in school.

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its networks, devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. The Online Safety Leader, working with the PET ITL Team is responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.
- The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These may include:
    - physical monitoring (adult supervision in the classroom)
    - internet use is logged, regularly monitored and reviewed
    - filtering logs are regularly analysed and breaches are reported to SLT
    - pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
    - school technical staff regularly monitor and record the activity of users on the school technical systems
    - use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring leads.

Audit / Reporting

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

- The Principal
- DSL
- 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.