St Pauls CE Primary School

Technical Security Policy Template

Written: Autumn 2024

Reviewed : Autumn 2025

Aims

This Technical Security Policy outlines the commitment of **St Pauls CE Primary School** to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Technical Security Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

It is the aim of this policy to provide details relating to effective technical security which includes filtering & monitoring. This is informed by the Department for Education (DfE) guidance, Keeping Children Safe in Education,

The school Governors and SLT who are further supported by the DSL/ IT Support are 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
- access to personal data is securely controlled in line with the school's personal data policy
- system logs are maintained and reviewed to monitor user activity
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision

Roles

- School technical systems are managed in line with the DfE's Digital and Technology Standards
- Cyber security is included in the school risk register. This is the responsibility of SLT.
- There will be regular reviews and audits of the safety and security of school technical systems.
- The school servers, wireless systems, and cabling are all securely located and physical access restricted.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud, Currently the school's procedures include 3 USB device changes by admin staff on Mon, Weds, Fri. In addition, daily cloud back up is also operational.
- Appropriate security measures (including updates) are in place 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, including operating systems.

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

- The responsibilities for the management of technical security are assigned to IT support/ SLT/Smoothwall via Stockport LA

- All users will have clearly defined access rights to school technical systems and accounts are deleted when the user leaves. *This will be recorded by school admin and reviewed, annually, by the SLT.*

- Adult 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 IT Service Provider, in partnership with SLT/DSL, regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.

- Mobile device security and management procedures are in place. These are *managed by Jamf and filtered via Stockport's Smoothwall.*

- An appropriate system is in place (CPoms) for users to report any actual/potential technical incident to the SLT/DSL.

- The school business manager/IT support 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.

- Guest users are provided with appropriate access to school systems based on an identified risk profile *by default, users do not have administrator access to any school-owned device.*

- *Guidance is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school. This can be seen in the Mobile Devices Policy.*

- **Guidance** is in place regarding the use of removable media by users on school devices. Currently, the school allows the use of USB pen drives. These are issued by the school and are encrypted. Personal USB devices are **not** allowed for use by school staff. Visitors **may** use USB pen drive with the permission of the headteacher, these must be scanned before use.

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

Password Security

At St Pauls CE Primary a safe and secure username/password system is in place and applies to all school technical systems, including networks, devices, email and learning platform.

- The password policy and procedures reflect NCSC and DfE advice/guidance.
- Security measures are in place to reduce brute-force attacks and common passwords are blocked.
- School networks and systems are protected by secure passwords.
- Passwords are encrypted by the system to prevent theft.

.

- Complexity requirements (e.g. capital letter, lower case, number, special character) are not used for children but are used for staff members.

- Adult users are able to reset their password themselves.
- All network passwords are at least 8 characters long for staff.
- Passwords are immediately changed in the event of a suspected or confirmed compromise.
- No default passwords are in use. All passwords provided "out of the box" are changed to a unique password by the IT Support at Stockport LA.
- All accounts with access to sensitive or personal data are protected by Multi-Factor Authentication methods.
- A copy of administrator passwords is kept in a secure location.
- All users (adults) 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 must not be shared with anyone.
-

- **Learner Passwords:**

All pupils are issued with a username and password in order to access the schools network. This stays with the pupil for the duration of their time at the school. Pupils have restricted access to the school network and currently are able to access designated shared drives these are listed below..

Home Area

Public Area

Get Work Here

Once a child leaves the school these accounts are archived/deleted.

For younger children and those with special educational needs, learner usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity for these users could be reduced (for example 6-character maximum) and should not include special characters

Curriculum
Learners will be taught the importance of password security, this includes how passwords are compromised, and why these password rules are important. This will be covered in the subjects below:

Computing

PSHE

RSE

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, as online content 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.

Process

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 broadband or filtering provider by actively employing the Internet Watch Foundation URL 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 use of technology at St Pauls Primary School includes PC's, laptops and iPads. Filtering is applied to all devices and is provided by the local authority technical services.

The schools filtering system is set up and applied to all:

- users, including guest accounts.
- school owned devices
- devices using the school broadband connection.

The filtering system is set up to complete the tasks below:

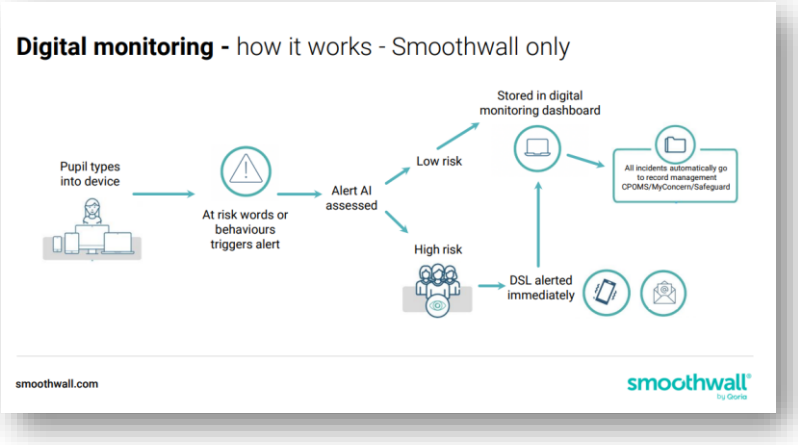
- Filter all internet feeds, including any backup connections.
- Is age and ability appropriate for the users and be suitable for educational settings.
- Can handle multilingual web content, images, common misspellings and abbreviations.
- Can identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.
- Provides alerts when any web content has been blocked.

Monitoring

Monitoring user activity on school devices is an important part of providing a safe environment for children/staff and allows the school to review user online activity. In order to take prompt action, the school have a monitoring system which alerts a designated member of staff who has the responsibility to deal with and log issues.

In order to further minimise safeguarding risks on internet connected devices, other monitoring process may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services



Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	?
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	Jo Harrington-Headteacher
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports	Jo Harrington

	• safeguarding concerns • checks to filtering and monitoring systems	
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	Stockport LA
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material	

Changes to Filtering and Monitoring Systems

There should be a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system.

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

Requests for changes to the filtering and monitoring system must be requested to the Headteacher/DSL. No changes must be made without this approval.

Once approved it is the responsibility of Stockport LA to make these changes and inform that Headteacher/DSL that these have been completed.

Commented [D1]: Change to Stockport LA

An audit of changes will be logged by SLT.

Filtering and Monitoring Review and Checklist

In order to understand and evaluate the changing needs and potential risks of the school, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by members of the SLT, the designated safeguarding lead (DSL), Stockport LA and the IT service provider. Additional checks to

filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

Commented [D2]: Stockport LA has been added

Reviewing the filtering and monitoring provision

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.

The review will take account of:

- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RSE and PSHE curriculum
- the specific use of chosen technologies
- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled

To make the filtering and monitoring provision effective, the review will inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review will be carried out as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, e.g. remote access or BYOD
- new technology is introduced

Checking the filtering and monitoring systems

Commented [D3]: Do you have responsibility for checking devices?

Checks to filtering and monitoring systems will take place termly. Checks will be undertaken from both a safeguarding and IT perspective.

Checks to the filtering and monitoring systems will include further checks to verify that the system setup has not changed or has been deactivated. Checks will be performed on a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

Logs of checks are kept so they can be reviewed. These record:

- when the checks took place
- who did the check
- what was tested or checked
- resulting actions

See table below:

Filtering & Monitoring Checks

Date of Check	Staff Member	What was tested/Checked	Resulting Actions

Backup

NCSC 3-2-1 backup solution is in place to ensure, Onsite, Offline and Offsite backup is in place, operational and monitored.

There is a process to check unsuccessful backup reports and rectify issues

Commented [D4]: Can you give exact details for the back up process as I know this is changing?

Security Measures

Data protection: All sensitive data is encrypted when stored or transmitted. Data backup and recovery procedures are in place to ensure data availability.

Network security: The education establishment's network is secured by firewalls and regularly monitored for security threats.

Mobile device security: All mobile devices which leave the school building are encrypted and have password protection. Lost or stolen devices must be reported immediately to SLT.

Software security: Only authorised software applications approved by SLT may be installed on technology systems. All software is kept up-to-date with the latest security patches.

Physical security: All technology systems are physically secured when not in use.

Incident response: The education establishment has a Buisiness Continuity plan in place to respond to security incidents and minimize potential harm.

CPD:

Safeguarding training is completed by all staff annually, this is carried out in the autumn term and is delivered by the DSL/SLT. In order to protect personal and sensitive data, governors, senior leaders, staff receive training about information security and data protection, annually.

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring (Responsible Governor, DSL, OSL or other relevant persons) will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons when using technology
- through the acceptable use agreements

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter / School Website etc.

Audit/Monitoring/Reporting/Review:

Governors/SLT/DSL will ensure that full records are kept of:

- Training provided
- User Ids and requests for password changes
- *User logons*
- *Security incidents related to this policy*
- *Annual online safety reviews including filtering and monitoring*
- *Changes to the filtering system*
- *Checks on the filtering and monitoring system*