Technical Security Policy (including filtering, monitoring and passwords)

DUKE OF NORFOLK CE PRIMARY SCHOOL

Approved by:	Full Governing Body	Date: Nov 2023
Last reviewed on:	Nov 2023	
Next review due by:	Nov 2025	

1 Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. This is informed by the Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards and therefore applicable for schools and colleges in England. For schools and colleges outside England, this would be considered good practice, the school should also ensure that they remain compliant with national, local authority or MAT guidance, as relevant. The school is responsible for ensuring that the 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 Data Protection 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

This policy is not designed to reproduce the entirety of the DfE's standards, but is designed to support governors and senior leaders in the production of a technical security policy. Governors and senior leaders remain responsible for the school's technical security.

2 Responsibilities

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management of technical security is the responsibility of Governors and Senior Leaders, supported in this by the Designated Safeguarding Lead, Online Safety Lead and IT Service Provider.

The school is 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 recommended technical requirements.
- Cyber security is included in the school risk register.
- 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.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- 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.
- 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 and accounts are deleted when the user leaves. Details of the access rights available to individual users will be recorded by the school administration 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.
- The IT Service Provider, in partnership with Governors/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 so that no personal devices can access the school network, and that no data relating to school is stored on personal devices.
- Users are to report any actual/potential technical incident to the SLT/DSL/Online Safety Lead or IT Service Provider
- The IT Service Provider/School administrators 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, as set out in the Online Safety Policy
- By default, users do not have administrator access to any school-owned device.
- An agreed policy (Online Safety) is in place regarding the extent of personal use that users (staff/learners) and their family members are allowed on school devices that may be used out of school.
- An agreed policy (Online Safety) is in place regarding the use of removable media by users on school devices.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

3 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 learning platform.

- The password policy and procedures reflect NCSC and DfE advice/guidance.
- The use of passwords is reduced wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO.
- Security measures are in place to reduce brute-force attacks and common passwords are blocked.
- School networks and system will be protected by secure passwords.
- Passwords are encrypted by the system to prevent theft.

- Passwords do not expire and the use of password managers is encouraged.
- Complexity requirements (e.g. capital letter, lower case, number, special character) are not used.
- Users are able to reset their password themselves.
- All passwords are at least 12 characters long and users are encouraged to use 3 random words.
- 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 Service Provider.
- All accounts with access to sensitive or personal data are protected by Multi-Factor Authentication methods, where possible.
- A copy of administrator passwords is kept in a secure location.
- All users (adults and learners) 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.

4 Learner Passwords

- Learners are encouraged to set passwords with an increasing level of complexity. Passwords using 3 three random words and with a length of over 12 characters are considered good practice.
- Users will be required to change their password if it is compromised.
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important. The ProjectEVOLVE Privacy and Security strand will help you with this.

5 Filtering and Monitoring

5.1 Introduction to 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. 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.

DfE Keeping Children Safe in Education requires schools to have "appropriate filtering". DfE published Filtering and monitoring standards for schools and colleges in March 2023. Schools are recommended to use the UK Safer Internet Centre Definitions to help them determine if their filtering system is appropriate.

We will test our filtering for protection against illegal materials at: SWGfL Test Filtering

Our filtering system should be operational, up to date and applied to all:

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

Our filtering system should:

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

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

5.2 Introduction to Monitoring

Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows us to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

Our monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and includes:

- physically monitoring by staff watching screens of users
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

5.3 Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools identify and assign roles and responsibilities to manage our 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.	David Mundy (Safeguarding Governor)
Senior Leadership	Team Member Responsible for ensuring these standards are met and:	Esther Bland (HT/DSL) Kellie Wilson (DHT/DSL)

	> 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	
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: > filtering and monitoring reports > safeguarding concerns > checks to filtering and monitoring systems	Esther Bland (HT/DSL) Kellie Wilson (DHT/DSL)
IT Service Provider	Technical responsibility for: > maintaining filtering and monitoring systems > providing filtering and monitoring reports > completing actions following concerns or checks to systems	Chris Player (Complink)
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	

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.

> There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
> There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
> Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
> The filtering and monitoring provision is reviewed at least annually and checked regularly.
> There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.

> 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.

5.4 Filtering and Monitoring Review and Checks

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 senior leadership team, the designated safeguarding lead (DSL), 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.

5.5 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 RHSE and PSHE curriculum
> the specific use of chosen technologies, including Bring Your Own Device (BYOD)
> 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

5.6 Checking the filtering and monitoring systems

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are 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

6 Training/Awareness:

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
- 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 etc. (amend as relevant)

7 Audit/Monitoring/Reporting/Review:

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

> Training provided

- User Ids
- 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 systems