TECHNICAL SECURITY POLICY

Contents

Contacts and Review Information

Data Protection Officer	dposchools@somerset.gov.uk
School Data Protection Lead	Matt Bowles
The policy was approved by Governors / Trustees on:	_____
Signature of Chair of Governors / Trustees:	_____
The next review date is:	_____

Version Control

Version	Author(s)	Date Produced	Amendments
2.0	SSE DPO	01/09/23	Significant changes to previous policy made to reflect updated DfE Digital and Technical Standards. New policy draws on updated SWGfL technical security policy.

Introduction

1.1 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 for Schools and Colleges.

1.2 The School is responsible for ensuring that school technical systems (network, infrastructure, devices) are 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 or business continuity purposes within the school's policies).
- 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 procedures
- there is oversight from senior leaders and this has an impact on policy and practice
- there is an up-to-date Business Continuity and Disaster Recovery Plan including the School response to a major cyber incident such as a ransomware attack which could significant impact the school's ability to deliver education, run the school site, and safeguard learners

1.3 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 has a contract with Computing Cubed to provide support for technical security
- It is the responsibility of the School to ensure that the provider complies with expectations in the Digital and Technology Standards. It is also important that the IT service provider works in partnership with the Designated Safeguarding Lead (DSL) to support the school safeguarding requirements.
- The School should also check that their managed service provider is following up-to-date guidance and advice from the National Cyber Security Centre https://www.ncsc.gov.uk/section/advice-guidance/all-topics

Scope of the policy

1.1 This policy should be read alongside the following School documents:

- Business Continuity and Disaster Recovery Plan
- Data Protection Policy
- Online Safety Policy
- Safeguarding Policy
- Privacy notices for pupils/parents

2.2 This policy reflects the requirements of the School to comply with the following legislation and statutory guidance:

- The UK General Data Protection Regulation
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- Keeping Children Safe in Education 2023
- Meeting digital and technology standards in schools and colleges

2.3 This policy applies to all staff including school, agency staff, contractors, work experience students and volunteers.

Responsibilities of the Trust/Academy/School

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.

The School will:

3.1 ensure that school technical systems are managed in ways that ensure that the school meets the Digital and Technology Standards

3.2 ensure that the relevant people receive up-to-date guidance (e.g. from the National Cyber Security Centre) and training and are effective in carrying out their responsibilities

3.3 ensure that there are regular reviews and audits of the safety and security of School technical systems (see Section 12 Monitoring)

3.4 ensure that servers, wireless systems and cabling are securely located and physical access restricted

3.5 ensure that appropriate security measures 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

3.6 by liaison with the network manager/technical support provider, ensure that all users have clearly defined access rights to school technical systems

3.7 by liaison with the network manager/technical support provider, ensure that details of the access rights available to groups of users are recorded by the network manager and are reviewed, at least annually, by the senior leadership team

3.8 by liaison with the network manager/technical support provider, ensure that an appropriate system is in place for users to report any actual/potential technical incident to the nominated in-school lead and Designated Safeguarding Lead, if appropriate

3.9 by liaison with the network manager/technical support provider, ensure that an agreed policy is in place and implemented 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 the school

3.10 by liaison with the network manager/technical support provider, ensure that an agreed policy is in place and implemented regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices

3.11 by liaison with the network manager/technical support provider, ensure that the school infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.

3.12 by liaison with the network manager/technical support provider, ensure that any cyber incidents are reported to the relevant authorities e.g. Action Fraud

Responsibilities of network manager/technical support provider

4.1 The responsibilities of the network manager are primarily listed in the Network Manager Job Description.

4.2 The responsibilities of the technical support provider are primarily listed in the contract with the provider.

4.3 In addition to the other requirements of this policy, the network manager / technical support provider will:

- Read, sign, and follow the School acceptable user agreement for technicians
- regularly monitor and record the activity of users on the school's technical systems (add details of the monitoring programs that are used)
- ensure 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)
- ensure that remote management tools are used by staff to control workstations and view users' activity
- ensure that mobile device security and management procedures are in place (where mobile devices are allowed access to School systems).
- ensure provision for temporary access of "guests", (e.g., trainee teachers, supply teachers, visitors) onto the school system
- enforce the School agreed policy regarding the downloading of executable files and the installation of programs on school devices by users

Responsibilities of staff

5.1 This policy applies to all staff including school, agency staff, contractors, work experience students and volunteers.

The School staff will:

- read, sign, and follow the School 's acceptable user agreement

- read and follow the School's Data Protection policy
- complete the National Cyber Security Centre's online staff training and maintain an awareness of the common types of security risks such as phishing and scam emails
- ensure that school devices are locked when the staff member is out of the room
- ensure that passwords for school systems are not shared with other staff members or students
- if using removable storage (laptop, tablet, USB memory stick) ensure that this is approved by the school, and is password protected and encrypted
- when working from home, ensure appropriate security is in place to protect equipment or information not be used by non-school staff. This will include ensuring equipment and information is kept out of sight
- ensure that any machine not routinely connected to the school network, is brought in regularly to receive updates by the IT team
- ensure that all school data is stored on the school network or portal, not kept solely on the laptop
- ensure that all locally stored data is synchronised with the school network server on a frequent basis
- ensure that school-issued laptops are available for inspection by school-authorised personnel (e.g. the network manager) at any time
- not attempt to access any network drives or areas to which they do not have authorised permission from the School
- not attempt to by-pass security to download apps or .exe files without the prior permission of the school
- use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code
- **in the event of a suspected cyberattack.** turn off device and inform the school office and do not connect device to the school network until it has been checked by the network manager

Network/Server security

6.1 Servers are physically located in an access-controlled environment. Unrestricted access to the computer facilities is confined to designated staff whose job function requires access to that particular area/equipment

6.2 Restricted access may be given to other staff or third-party support where there is a specific job function need for such access

6.3 The most recent security patches are installed on the system as soon as practical. The only exception being when immediate application would interfere with business requirements

6.4 Servers will have security software (Anti-Virus and Anti-Spyware) installed appropriate to the machine's specification and in line with current recommendations from the National Cyber Security Centre https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software

6.5 Servers will always be password protected, and locked when not in use

6.6 Users will not be able to download apps or .exe files without the prior permission of the school and network manager/technical support provider

6.7 Security-related events should be reported to the IT team and to the DPO. Corrective measures will be prescribed as needed. Security-related events could include, but are not limited to, port-scan attacks, evidence of unauthorised access to privileged accounts

6.8 IT infrastructure such as routers, switches, wireless access points etc. should be kept securely and only be handled by authorised personnel

6.9 Backup Procedures:

- Backup software must be scheduled to run routinely, as required, to capture all data as required
- Backups should be monitored to make sure they are successful
- A test restoration process will be run regularly and at least annually (see Section 12 Monitoring)
- Backup media must be securely stored in a fireproof container
- Backup media stored off-site must be transported and stored securely

Workstation security

7.2 Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information is restricted to authorised users, including:

- restricting physical access to workstations to only authorised personnel
- securing workstations (screen lock or logout) prior to leaving area to prevent unauthorised access
- enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected
- complying with all applicable password policies and procedures
- ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- ensuring workstations are used for authorised purposes only
- never installing unauthorised software on workstations
- storing all confidential information on network servers
- keeping food and drink away from workstations in order to avoid accidental spills

Password security

Staff passwords

8.1 All school networks and systems are protected by secure passwords.

8.2 When working away from the school, staff will use multi-factor authentication to access the school's online resources.

8.3 All users have clearly defined access rights to school technical systems and devices. Details of the access rights available will be reviewed, at least annually, by the senior leadership team as detailed in Section 3.9

8.4 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

8.5 Passwords must not be shared with anyone

8.6 Passwords should be long. Good practice highlights that passwords over 12 characters in length are more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack

8.7 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

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

8.9 Passwords must be changed on first login to the system

8.10 Passwords should not be set to expire as long as they comply with the above but should be unique to each service the user logs into.

Learner passwords

8.11 Foundation Stage and KS1 learners will have simple passwords with a six-character maximum, without special characters

8.12 Records of learner usernames and passwords for Foundation Stage/KS1 pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.

8.13 Password requirements for learners at Key Stage 2 and above will increase as pupils progress through the School

8.14 All learners will be required to change their password if it is compromised. Passwords will not be regularly changed but should be secure and unique to each account.

8.15 Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Administrator passwords

8.16 Each administrator will have an individual administrator account, as well as their own user account with access levels set at an appropriate level. These accounts will have multi-factor authentication in place

8.17 Administrator passwords for the School systems should also be kept in a secure place. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account. (A school should never allow one user to have sole administrator access)

8.18 If the school uses any password manager tools for storing administrator passwords, they must follow the guidance from the National Cyber Security Centre on password

manager solutions https://www.ncsc.gov.uk/collection/passwords/password-manager-buyers-guide

Setting and resetting passwords

8.19 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.

8.20 Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by the network manager. The password generated by this change process should be system generated and only known to the user. This password should be temporary, and the user should be forced to change their password on first login. The generated passwords should also be long and random

8.21 Where automatically generated passwords are not possible, then an age-appropriate password generator e.g. www.dinopass.com or https://passwordsgenerator.net should be used to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary, and the user should be forced to change their password on the first login

8.22 Requests for password changes should be authenticated by the network manager to ensure that the new password can only be passed to the genuine user

8.23 Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use. (For example, providing a pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)

8.24 In good practice, the account is “locked out” following six successive incorrect log-on attempts

8.25 Passwords shall not be displayed on screen and shall be securely hashed when stored (use of one-way encryption)

Filtering and monitoring

Introduction to Filtering

9.1 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 provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

9.2 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.

9.3 The school should also ensure that filtering is balanced against learning needs to reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies

9.4 DfE Keeping Children Safe in Education requires schools to have "appropriate filtering". The DfE published Filtering and monitoring standards for schools and colleges in March 2023.

9.5 The School filtering system is applied to all:

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

9.6 The School filtering system will:

- 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

Introduction to Monitoring

9.7 Monitoring user activity on School 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 the School to review user activity on school and college 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.

9.8 A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and 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

9.9 DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage 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.	Debbie O'Sullivan
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	Matt Bowles
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	Claire Marsland
IT Service Provider	• Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	Computing Cubed
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns.	• 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	

They should report if:	• 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	

Filtering and monitoring at the School

9.9 Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.

9.10 There is a filtering system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content. Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school.

9.11 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.

9.12 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.

9.13 There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.

Changes to the Filtering and Monitoring Systems

9.14 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.

9.15 Users may request changes to the Designated Safeguarding Lead (DSL).

9.16 The DSL will, in connection with the Online Safety Lead, assess whether the change is:

- appropriate to the school's responsibilities under Keeping Children Safe in Education
- permitted or denied

9.17 The DSL will record the changes to the filtering and monitoring system and the school's decision-making process.

Filtering and Monitoring Review and Checks

9.18 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 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.

9.19 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

9.20 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

9.21 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

9.22 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.

9.23 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

9.24 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

Awareness and training

9.1 It is essential that users are aware of the need to keep the school's systems safe from harm.

9.2 This will be done at an age-appropriate level e.g., for young learners, staff will talk about the importance of keeping your password safe (see the Online Safety policy for further details). Key Stage 2 learners will complete the National Cyber Security Centre's CyberSprinters activity https://www.ncsc.gov.uk/collection/cybersprinters

9.3 Staff will complete the National Cyber Security Centre School Training https://www.ncsc.gov.uk/information/cyber-security-training-schools

9.4 It will also be done through staff modelling appropriate use e.g., not leaving devices logged on, and not sharing passwords with classroom assistants

9.5 Members of staff will be made aware of this policy:

- at induction
- when logging onto the school network
- through the online safety policy and password security policy
- through the acceptable use agreement

9.6 Learners will be made aware of this policy:

- when logging onto the school network (via an age-appropriate login message)
- in lessons (e.g. online safety lessons)
- through the acceptable use agreement

Disposal of Redundant ICT Equipment

10.1 All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

10.2 All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. The School will only use authorised companies who will supply a written guarantee that this will happen.

10.3 Disposal of any ICT equipment will conform to:

- the Waste Electrical and Electronic Equipment Regulations 2018
- the UK GDPR and Data Protection Act 2018
- the Electricity at Work Regulations 1989

10.4 The School will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. This will include:

- Date item disposed of
- Authorisation for disposal, including: verification of software licensing, any personal data likely to be held on the storage media
- How it was disposed of e.g. waste, gift, sale.
- Name of person and/or organisation who received the disposed item.

10.5 Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Reporting policy incidents

11.1 Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data should raise the matter with the Headteacher.

Monitoring and evaluation

12.1 This policy will be monitored and reviewed in line with the School's policy review procedure.

12.2 The School will monitor the implementation of the policy through:

- maintaining an up-to-date business continuity plan that reflects the latest risks to education settings following advice from the National Cyber Security Centre
- checking the school's technology standards against the latest DfE guidance https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
- annual data protection walks around the school site to ensure that the school's requirements are followed by staff
- annual back-up and restore check of data
- regular spot checks of school systems and devices
- checks against national cyber security auditing systems e.g. the Cyber Essentials scheme About Cyber Essentials - NCSC.GOV.UK