Squirrel Hayes First School

Policy Reviewed on	March 2021	March 2022	March 2023	March 2024	March 2025	March 2026
Policy Owner Signature	Mrs R Percival	Mrs R Percival	Mrs R Percival	Mrs R Percival	Mrs R Percival	Mrs R Percival
Policy adopted by the Governing Body on	March 2021	March 2022	March 2023	March 2024	March 2025	March 2026
Policy to be reviewed on	March 2022	March 2023	March 2024	March 2025	March 2026	March 2027
Version	01	02	03	04	05	06

Technical Security Policy

Introduction

The purpose of this Technical Security Policy is to ensure the school's ICT infrastructure, data, devices, and digital services are protected against internal and external threats—whether deliberate or accidental. The school aims to safeguard confidentiality, integrity, and availability of information at all times. This policy is informed by **Department for Education (DfE) guidance**, including *Keeping Children Safe in Education* and the *Digital and Technology Standards*.

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school 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 or to share resources).
- Access to personal data is securely controlled in line with the school's personal data 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 computer 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 ICT Technician and SLT.

Scope

This policy applies to:

- All staff, governors, volunteers, contractors, and authorised ICT users.
- All devices used for storing or processing school data, including workstations, servers, mobile devices, and cloud-based systems.

Technical Security

Policy statements

Squirrel Hayes will be responsible for ensuring that the school 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
- There will be regular reviews and audits of the safety and security of school academy 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 ICT Technician and will be reviewed, at least annually, by the SLT
- 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.
- School Burser / ICT lead 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
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential technical incident to the ICT Technician (or other relevant person).
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc

- Personal data cannot 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 networks, devices, email and Virtual Learning Environment (VLE).

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 ICT Technician (or other person) and will be reviewed, at least annually, by the SLT.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- All users (adults and young people) 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 school admin staff.
- Where passwords are set / changed manually requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user.

Staff passwords:

- All staff users will be provided with a username and password. Staff members then choose their own password.
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on

Student / pupil passwords

- All users will be provided with a username and password and these will be recorded.
- Students / pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

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

- At induction
- Through the school's online safety policy
- Through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- In lessons
- Through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person will ensure that full records (manual or automated) are kept of:

- User Ids and requests for password changes
- User log-ins
- Security incidents related to this policy

Protection Against Cyber Threats

Threats may include malware, ransomware, phishing, and denial-of-service attacks. Schools must ensure:

- Staff receive regular cyber-security training.
- Suspicious emails and attachments are not opened.
- Staff verify the sender and legitimacy of digital communications.

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.

Responsibilities

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- be logged in change control logs
- be reported to a second responsible person
- either... be reported to and authorised by a second responsible person prior to changes being made.

All users have a responsibility to report immediately to the Headteacher and the ICT 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 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 the Internet Service Provider.
- Any filtering issues should be reported immediately to the filtering provider.

Education / Training / Awareness

Learners will be made aware of the importance of filtering systems through the online safety education programme. 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 Acceptable Use Agreement
- Induction training
- Staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.

Filtering & Monitoring

- The school uses robust filtering to prevent access to harmful content.
- Monitoring tools are used to track activity for safeguarding and security purposes.
- Regular reviews and audits ensure these systems remain effective.

Technical Infrastructure, Filtering and Monitoring

The Head teacher will be responsible for ensuring that Squirrel Hayes' school network infrastructures are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Our schools also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Technical systems will be managed in ways that ensure that the schools meet recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to technical systems and devices.
- All users will be provided with a username and secure password by the ICT Support Team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" password for schools ICT system as used by the ICT Leader (technical) must also be available to the Headteacher and kept securely in the school safe.
- The ICT 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.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests

for filtering changes.

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy (AUP).

- The active monitoring system employed in school is regularly updated to flag up a range of key words and phrases, for example, it contains a range of radicalisation words and phrases. This enables full visibility of any possible exposure to harmful content and radicalisation happening within the network.

- Due to the dynamic and changing nature of language, our filtering/monitoring solution provider liaises with a range of expert agencies and partners to ensure that our libraries use up-to-the minute words and phrases that reflect contemporary digital activity. Our libraries are therefore reviewed and updated by our provider on an on-going basis. This aids us in ensuring that pupils are protected from terrorist and extremist influences.

- A Safeguarding and Child Protection Incident system is in place for users to report any actual or potential online safety incident. Staff can obtain a Safeguarding and Child Protection Incident Form from , and must complete and submit this form to an Online Safety Lead or DSL for investigation/follow up within ten minutes of an incident.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the schools systems and data. These are tested regularly. Schools infrastructures and individual workstations are protected by up to date anti-virus software.

- Temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems is subject to their agreement to the Staff Acceptable Use Policy (AUP).

- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users).

- The Schools Data Protection Policy covers the use of removable media such as memory sticks, CDs and DVDs by users on school devices. The policy stipulates that whilst any USB memory sticks may be used on school systems for the reading of data, data from school systems will only be writeable to school owned and encrypted USB memory sticks. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (see Data Protection Policy for more). For more details, see the Technical Security Policy.

Further Guidance

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore the Department for Education published proposed changes to 'Keeping Children Safe in Education' for consultation in December 2015. Amongst the proposed changes, schools will be obligated to *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system"* however, schools will need to *"be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*

In response UKSIC produced guidance on – information on "Appropriate Filtering"

NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/

This checklist is particularly useful where a school / academy uses external providers for its technical support / security: https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx

DOCUMENT CHANGE LOG

Version No.	Date of review	Reviewer	Changes Made
01	March 2021	Mrs Percival	New policy based on New GDPR rules
02	March 2022	Mrs Percival	Reviewed
03	March 2023	Mrs Percival	Reviewed no changes made
04	March 2024	Mrs Percival	Filtering and monitoring updated.
05	March 2025	Mrs Percival	Reviewed no changes made

Version No.	Date of review	Reviewer	Changes Made
06	March 2026	Mrs Percival	Addition of information in the introduction and scope. Addition of filtering and monitoring. Addition of cyber threats.