Technical Security Policy

St Eanswythe's Church of England Primary School

Learning holistically through God's unconditional love

We radiate God's unconditional love by being accepting, inclusive and supportive. Everyone is nurtured, enabling them to reach their full potential as caring, confident members of both the school family and global community. All are educated holistically through a variety of enjoyable academic, creative, physical and spiritual experiences.

Date: **September 2024**

Signed: **Headteacher**

Signed: **Chair of Directors**

Technical Security Policy (including filtering and passwords)

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 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).
- 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 headteacher.

Technical Security

Policy statements

The school 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 recommended technical requirements
- 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
- all users will have clearly defined access rights to school technical systems
- 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 headteacher 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
- *Managed service provider 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 Safeguarding Team.*
- A limited access 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 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*
- An agreed policy is in place regarding the use of removable media (e.g. 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, e-mail and learning platform. Where sensitive data is in use – particularly when accessed on mobile devices – schools may wish to use more secure forms of authentication e.g. two factor authentication.

Policy Statements:

- These statements apply to all users.
- All school networks and systems will be protected by secure passwords.
- All users 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 Managed Service Provider and will be reviewed, at least annually.
- 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.
- All users will be provided with a username and password by the managed service provider who will keep an up to date record of users and their usernames.

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably 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.
- 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 the 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.

Learner passwords:

- Records of learner usernames and passwords for foundation phase learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- Password requirements for learners at Key Stage 2 and above should increase as learners progress through school.
- 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.

Notes for technical staff/teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts.
- An administrator account password for the school 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. Other administrator accounts should not have the ability to delete this account.
- 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.
- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by the Managed Service Provider
- Other than the user themselves, requests for password changes should be authenticated the senior leadership team 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 which expire after use.
- In good practice, the account is "locked out" following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

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

- at induction
- through the Technical Security Policy
- through the acceptable use agreement

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

- in lessons by their teacher
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:
The Managed Service Provider will ensure that full records are kept of:

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

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

The responsibility for the management of the school's filtering policy will be held by the Designated Safeguarding Leads. 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 logged in change control logs
- be reported to a second responsible person: Headteacher.

All users have a responsibility to report immediately to the Designated Safeguarding Leads. 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
- The school has provided enhanced/differentiated user-level filtering through the use of the Watchguard filtering programme (allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.)
- 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 Headteacher (or other nominated senior leader).
- Mobile devices that access the school 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.

Education/Training/Awareness

Learners will be made aware of the importance of filtering systems through the online safety education programme NCSC. 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
- their employee handbook

- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the acceptable use agreement..

Changes to the Filtering System

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/equipment as indicated in the school Child Protection and Safeguarding Policy and the acceptable use agreement.

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to the Designated Safeguarding Leads and:

- Governors committee/Management Committee member for child protection
- 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.

IT Security Systems Tracker

System	Location of System (on premise or cloud)	Password Complexity Settings	MFA Status	IP Address Setup as Trusted Site (no MFA prompt)	Risk Level (High / Low)
e.g. Office 365	e.g Cloud	e.g. 8 characters, 1 special, 1 capital	e.g. Enabled	e.g. 1.1.1.1	e.g. Low