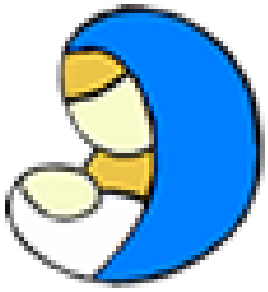
St Mary's RC Primary School



Technical Security Policy

Date policy reviewed: January 23

Reviewed: May 2024

To be reviewed: May 2025

Signed by:

D Hayes Headteacher
L Gillies Chair of Governors

School Mission Statement

'We Care, We Pray, We Work, We Play, in Jesus' way…'

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 ICT Lead Subject Co-ordinator.

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
- the schools wireless network is compliant with the KCSIE and DfE standards. It involves a guest wireless network with a unique password. This enables devices to be identified by SICT thus reducing the risk of allowing potentially unfiltered access in school.
- 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
- 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 network manager/technical staff/other person and will be reviewed 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 ICT Lead Subject Coordinator 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 Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.
- *mobile device security and management procedures are in place* where mobile devices are allowed access to school systems. An example of this may be the schools email system which requires 2 step authentication.
- an appropriate system is in place for users to report any actual/potential technical incident to the online safety co-ordinator/network manager technician (or other relevant person, as agreed). Staff are able to speak with the ICT Lead or any member of the school's SLT to report any concerns or incidents which may arise.
- as per school practice, only long term regular visitors are given temporary access as "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school's systems
- downloadable, executable files and the installation of programmes on school devices is implemented by a representative from SICT.
- school users are aware that their family members are not permitted to use their school devices without prior permission. When working from home, staff must use remote access to work on school held information.
- pen drives must not be used unless in exceptional circumstances and then it must be an encrypted one.
- the school's 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 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.

Further guidance can be found from the National Cyber Security Centre and SWGfL "Why password security is important"

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 Network Manager (or other person) 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 school office staff 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. A strong password policy has been agreed with schools and deployed by SICT.
- 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.
- 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:

Learners are given unique usernames and passwords to access the pupil drive in school. This is generated by SICT. In this way, pupils should always be supervised and members of staff should never use a class log on for their own network/internet access.

- Records of learner usernames and passwords are kept in paper-based form, but they are securely kept when not required by the user.
- Password requirements for learners at Key Stage 2 and above increase as learners progress through school.
- Users will be required to change their password if it is compromised to ensure they are unique and secure to individual accounts.
- 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 has 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.
- SICT oversee the Administrator account function for subscribing schools. School also has a local administrator 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 school office or SICT.
- Requests for password changes should be authenticated by the school office staff to ensure that the new password can only be passed to the genuine user
- Visitors are provided with appropriate access to systems which expires after use.
- In good practice, the account is “locked out” following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen.

Training/Awareness:

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users. It is also essential that users be taught how passwords are compromised, so they understand why things should be done a certain way. Please see our blog for more details on this.

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

- at induction
- through the school online safety policy and password security policy
- through the acceptable use agreement

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

- in ICT lessons
- through the pupil e-safety/online safety agreement for each key stage

Audit/Monitoring/Reporting/Review:

The school’s ICT Lead Co-ordinator 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 SICT. 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.

All users have a responsibility to report immediately to the ICT Lead Co-ordinator 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.

- SICT maintains and supports the managed filtering service
- SICT provides enhanced/differentiated user-level filtering through the use of Active Directory
- 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
- Any filtering issues should be reported immediately to SICT.

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

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

Changes to the Filtering System

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

- The school ICT Lead Coordinator or SBM/HT can request changes via SICT helpdesk
- SICT will provide checks and balances

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the ICT Lead Co-ordinator who will decide whether to make school level changes (as above).

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 and on school equipment as indicated in the school online safety policy and the acceptable use agreement. Monitoring will be the responsibility of all staff when with learners, but overse3en by the ICT Lead Co-ordinator.

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person
- Online Safety Group
- Online Safety Governor/Governors committee
- 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. The evidence might show a large number of requests to remove the filtering from sites – in which case school may question whether the current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring/disciplinary action might be necessary.

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).

The Department for Education ‘Keeping Children Safe in Education’ requires schools 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”