Simonside Primary School

Technical Security Policy

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 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 personal 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 using the system.
- There is effective guidance and training for users.
- There are 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 is the responsibility of IT Support (LA), Technical Staff.

Technical Security

Policy Statements

The school will be responsible for ensuring that their network and general infrastructure 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.

- 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 technical staff and shared appropriately only with other relevant school staff.
- 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.
- Helen Ross-Bell 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.
- School technical staff monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual or potential technical incident to the Online safety Lead.
- 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 extent of personal use that users and their family members are allowed on school devices that may be used outside of the 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 and 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 platforms. Where sensitive data is in use, the school will use two factor authentication as a more secure form of 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 Network Manager and will be reviewed at least annually.
- All users (adults and students) 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 relevant member of staff who will also 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 school/academy
- 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 can be kept in paper form as well as electronic form as long as they are stored securely when not required by the user.
- Password complexity for Early Years and Key Stage 1 should be reduced and not include special characters.
- Password requirements for students at Key Stage 2 should increase as they progress throughout school.
- Users will be required to change their passwords if password security is compromised.
- Passwords for external systems which have different password requirements should include random words and/or number combinations.
- Learner passwords must only be shared with relevant adults.
- Students will be taught the importance of passwords and password security as part of the Digital Literacy Curriculum.

Password notes for technical staff

- 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. This account and password should only ever 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. Message Digest algorithms should not be used.
- Suitable arrangements should be in place to provide visitors with appropriate access to systems.
- 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).

Password Awareness and Training

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.

Members of staff will be made aware of the school's Password Policy in the following ways:

- At general induction
- Through the school's Online Safety Policy and Password Security Policy
- Through the acceptable use agreement

Students will be made aware of the school's Password Policy:

- In Digital Literacy lessons
- In other lessons when/where appropriate
- Through assemblies
- Through online learning platforms
- Through the acceptable use agreement

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 IT Support (LA). This technical team 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, 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, the DHT

All users have a responsibility to report immediately to the DHT 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 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 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.

Awareness

Students will be made aware of the importance of filtering systems through the general computing and Digital Literacy curriculum. As part of this education, students will also be made aware 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
- General Induction training
- Relevant staff meetings and further CPD

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

Any changes to the filtering system will be in line with Local Authority and/or technical support team guidance.

Other changes may be requested as/when appropriate by members of staff. However, not all filtering requests may be permitted. The grounds on which filtering requests will be allowed or denied will be agreed by the DHT in conjunction with the technical team.

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.

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

- The second responsible person, the DHT
- Governors
- The external Filtering provider and/or the Local Authority
- The police, upon 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.

Policy Updated: October 2023

To be reviewed: October 2024