Be your best self

EXHALL GRANGE

SPECIALIST SCHOOL

School Technical Security Policy Editing (including Filtering and Passwords)

Responsible Staff	GG/RH
Governors Committee Responsible	Full Governing Board
Date Approved	September 2022
Review Date	Annually

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 Mr R Howlett (ICT Network Manager) and for PCE and Smoothwall systems management is carried out by Warwickshire ICTDS.

Technical Security – Policy statements

The school 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 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, workstations, 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 Network Manager and will be reviewed, at least annually, by Senior Leadership Team.
- 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.

- Mr R Howlett 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 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. Policy Central Software will be installed on all school terminals
- Remote management tools (NET Support) is used by staff to control workstations and view users activity
- An appropriate system is in place via the ICT portal for users to report any actual / potential technical incident to the ICT Network Manager.
- An agreed policy is in place using temporary account details 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 within group policies regarding the downloading of executable files and the installation of programmes on school devices by users is not permitted by these policies.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / 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, 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 Network Manager and will be reviewed, at least annually, by the Online Safety Group (or other group).
- All school networks and systems will be protected by secure passwords that are regularly changed
- The “master / administrator” passwords for the school / academy systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.
- 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 Mr R. Howlett ICT Network Manager, Teaching staff may change pupil passwords only. Any changes carried out to password integrity must be notified to the manager of the password security policy.
- Passwords for new users and replacement passwords for existing users will be issued through an automated process which includes provision of welearn365 account and school login credentials.
- Users will change their passwords at regular intervals – as described in the staff and pupil sections below
- 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 by Mr R. Howlett who will keep an up-to-date record of users and their usernames only.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- the account should be "locked out" following six successive incorrect log-on attempts
- 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
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- 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 for staff should be changed at least every 90 days.
- Passwords should not be able to be re-used for 6 months and be significantly different from previous passwords created by the same user. The last four passwords cannot be re-used.

Pupil Passwords

- **All users will be provided with a username and password** by Mr R. Howlett who will keep an up-to-date record of users and their usernames.
- Users will not be required to change their password unless they have a concern another person may know it due to the difficulties our pupils have with remembering information
- 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 and password security policy
- through the Acceptable Use Agreement

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

- in lessons via the allocated teaching time in each Key Stage.
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person Mr R. Howlett will ensure that full records are kept of:

- User IDs and requests for password changes
- User logins
- 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 Mr R. Howlett. He has responsibility to liaise with ICDTS to manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.
In addition, a report of concerns is generated for the internet safety officer daily to flag any searches or web sites that have been denied.

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

- be reported to a second responsible person Mr G. Goode Internet Safety Officer.

All users have a responsibility to report immediately to Mr R. Howlett 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 Smoothwall via the ICDTS the Service Provider

The school has provided differentiated user-level filtering through the use of the Smoothwall filtering programme. (allowing different filtering levels for different groups of users – staff / pupils 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.

- 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.
- Requests from staff for sites to be removed from the filtered list will be considered by Mr R. Howlett (ICT Network Manager) and Mr G. Goode (Internet Safety Officer). If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme in assemblies and timetabled ICT lessons. 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.

Changes to the Filtering System

The school operates a “Smoothwall” filtering system as part of the provision from ICDTS for all internet traffic connections via the school’s network.

In addition, the school terminals are also monitored by Policy Central as part of the provision with ICDTS.

The school also has NET Support software installed on curriculum machines for Teaching staff to be able to monitor and control pupil terminals.

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 Mr R. Howlett or Mr G. Goode 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.
Smoothwall is used to monitor Internet traffic.

Policy Central is used to monitor language and communications on school-based terminals
NetSupport is used to monitor the usage, activity and allows for remote connections by staff to pupil terminals.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to: Mr R. Howlett

- the second responsible person Mr G. Goode
- 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.