Cyber (Technical) Security Policy

Southend High School for Girls Academy Trust

Southend High School for Girls Academy Trust

Governor Policy 31NS	**Author: Sally Brierley**	**Authorised by: Board of Governors**
Cyber (Technical) Security Policy	**Date first issued April 2022**	**Page 2 of 8**

Reviewing authority: Student & Curriculum

Date for review	Reviewed Annually by	Reviewed by Board	A	B	C	Date of new edition
May 2022	Full Governors	24/05/2022			*	24/05/2022

A = accepted with no amendments

B = accepted with amendments

C = new edition created

Cyber (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 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 Data Protection policy
- Impero 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.
- there is effective anti-virus

Responsibilities

The management of cyber and technical security will be the responsibility of IT Manager, Director of Finance and Business and Headteacher. The IT strategy group (IT Manager, Director of Finance and Business) will monitor and review the cyber (technical) security, the group will expand to include students, safeguarding lead and a governor.

Cyber (Technical) Security

The school will be responsible for ensuring that their 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:

Policy statements for Cyber (Technical) Security

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements by the National Cyber security centre.
- there will be regular reviews and audits of the safety and security of school technical systems including day to day monitoring
- 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 IT manager.
- 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 (see ICT Acceptable user and Online Safety Policies)

- The IT Manager 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 (the Mobile Phone Policy).
- The technical staff regularly monitor and record the activity of users on the school technical systems with Impero 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 or potential cyber technical incident to the online safety co-ordinator/IT manager/technician or other relevant person, as agreed
- 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 with the use of guest and visitor logins.
- an agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users. Only school IT administrators can run .exe files for security reasons.
- An ICT Acceptable User 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
- the use of removable media (e.g. memory sticks/CDs/DVDs) is checked by anti-virus software.
- the school infrastructure and individual workstations are protected by up-to-date software by Intercept X which is a cloud-based solution to protect against malicious threats from viruses, worms, trojans etc. and by maintaining security updates as they are released.
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured, e.g. Encrypted offline files.

Password Security

A safe and secure username system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email, Office 365 and SMHW. See link to find out more about passwords, why they are important and how to manage them in this article Password Management & Security Guide | SWGfL. You may wish to share this with staff members to help explain the significance of passwords as this is helpful in explaining why they are necessary and important.

Policy Statements for Password Security:

- 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 IT Manager (or other person) and will be reviewed, at least annually, by the IT Strategy group.
- 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 IT Support who will keep an up-to-date record of users and their usernames by using Active Directory Users and Computers.

Password requirements:

- Passwords should be long. School protocol and good practice highlights those 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
- 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
- The school may wish to recommend to staff and students that they make use of a 'password safe' these can store passwords in an encrypted manner and can generate very difficult to crack passwords.
- Passwords should not be set to expire as long as they comply with the above but should be unique to each service the user logs into.
- Students will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important as part of online safety teaching.

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. Two factor authentication is used 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. Password Safe uses the Twofish encryption.
- It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by the IT Support team. This password is temporary, and the user is forced to change their password on first login. The new passwords are required to be long and complex.
- Suitable arrangements should be in place to provide visitors with appropriate access to systems, the guest users should be enabled and then disabled after use.
- In good practice, the account is "locked out" following five successive incorrect log-on attempts.
- Passwords shall not be displayed on screen or written down.

Training/Awareness:

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

- at induction
- through the acceptable use agreement

Students will be made aware of the school's password protocol:

- in lessons e.g. computer science or PHSEE lessons
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The IT Manager will ensure that full records are kept of:

- User Ids
- 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 strategy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school using the software Impero.

Many users are not aware of the flexibility provided by many filtering services at a local level for schools. Where available, schools should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies by use of a whitelist. Staff and Sixth form may request that a site be put in the whitelist for educational reasons.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by IT Manager. 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 recorded in the IT Support planner and be reported to the IT Strategy Group every month in the form of an audit of the change control logs.

All users have a responsibility to report immediately to the IT Manager 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 or security systems in place to prevent access to such materials.

Policy Statements for filtering

Internet access is filtered for all users. Differentiated internet access is available and customised filtering changes are managed by the school. Illegal content is filtered by the broadband provider Glide on a managed firewall 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 Glide, with a managed firewall
- The school manages its own filtering service via Impero and Exchange Online Protection.
- The school has provided enhanced or differentiated user-level filtering using the Impero filtering programme, which can allow different filtering levels for different Key Stages and different groups of users – staff/pupils/exams 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 will be subject to the same filtering standards as other devices on the school systems, personal devices will be protected by the firewall.
- Any filtering issues should be reported immediately to the IT Support team.

Education/Training/Awareness

Students will be made aware of the importance of filtering systems through the Acceptable Use Policy for Students. 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 training.

Parents have access to our filtering system by reading a copy of the Acceptable Use Policy on the school website.

Changes to the Filtering System

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

- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff IT Support team. If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly by the IT Strategy Group.
- The IT Support team will ensure the filtering system is up to date and relevant.

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 IT Manager will decide whether to make school level changes (as above).

Monitoring

The school uses server access logs and Impero logs to monitor all users who access the network.

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.

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to SLT upon request and

- IT Strategy 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.

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 Prevent duty guidance - GOV.UK (www.gov.uk)

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"

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed SWGfL Test Filtering