School Technical Security Policy Template (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 data protection 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 school with guidance from SIPS IT

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
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (this may be at school, local authority or managed provider level)
- 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 Technician and will be reviewed, at least annually, by SIPS IT. It is the schools responsibility to inform SIPS IT of required changes to access rights.*
- 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 password section below)*

- The school are responsible, with guidance from SIPS IT, 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).
- SIPS IT – the managed service provider manage the creation of policies to record log on and log off activity of users on the school domain controller and can be accessed upon request by SLT 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 agreed strategy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school's systems
- *only the school administrator for SIPS IT is allowed to download executable files and install such programmes on school devices*
- an agreed policy is in place (Online Safety) 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) by users on school devices is not allowed unless approved by SLT.
- 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). You can find out more about passwords, why they are important and how to manage them in our blog article. 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:

- 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 SIPS IT upon request and will be reviewed, at least annually, by the school. It is the schools responsibility to inform SIPS IT of required changes to access rights.
- All users 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 SIPS IT. An up to date record of users and their usernames are kept on the server.

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
- 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
- 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.

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 complexity in foundation phase should be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.
- 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 schools systems should also be kept in a secure place e.g. school safe. (Administrator access is only allowed by SIPS IT and is kept offsite)
- Administrator passwords stored digitally in SIPS IT should be securely managed behind a multi-factor authentication (MFA) login system, ensuring they are not stored on-site at the school in plaintext
- 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 SIPS IT. Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and

the user should be forced to change their password on first login. The generated passwords should also be long and random.

- Where automatically generated passwords are not possible, then a good password generator should be used by SIPS IT to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.
- Requests for password changes should be authenticated by the School Business Manager or Head teacher 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 expires after use. Pre-created user/password combinations that can be allocated to visitors should be recorded in a log, and deleted from the system 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 password policy:

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

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

- in lessons
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:
The responsible person, SIPS IT, will ensure that request records are kept of:

- User IDs and requests for password changes are logged in SIPS IT's CRM
- User logons (on Domain Controller via Audit Policy)
- Security incidents related to this policy are logged in SIPS IT's CRM

Filtering

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 LGFL and the ICT Co-ordinator. 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 (Head teacher):

All users have a responsibility to report immediately to SIPS IT or LGFL 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.

- *Either - The schools maintains and supports the managed filtering service provided by SENSO*
- *The school has provided enhanced/differentiated user-level filtering through the use of the* SENSO *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'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 the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by SIPS IT and the ICT Co-ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.*

Education/Training/Awareness

Learners will be made aware of the importance of filtering systems through the online safety policy. 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 policy.

Changes to the Filtering System

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 SIPS IT and/or the ICT 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 take place using the school access to SENSO*

Audit/Reporting

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

- the second responsible person School Business Manager
- Online Safety Governor/Governors resource 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"* (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"

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