TECHNICAL SECURITY POLICY

Together, we learn, love and grow with Jesus

Written by: R Jackson

To be reviewed: Autumn 2024

School 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 St. Jude's 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 Roisin Jackson (DHT, Computing Lead) and Angela Shaw (business manager), supported by MGL.

Technical Security

Policy statements

St. Jude's is responsible for ensuring that our infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We will 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.
- 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

- Angela Shaw 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* (refer to the Online Safety policy for more information)
- Smoothwall 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. Any concerns are immediately sent to the school's DHT which are then passed onto the MGL helpdesk to investigate. These are always given top priority.
- an appropriate system is in place for users to report any actual/potential technical incident to the computing/online safety lead or HT. This is called the 'Responding to incidents of misuse/Illegal incidents – flow chart.' Users are also aware that any technical difficulties can be reported to the MGL helpdesk.
- temporary access is also set up for the provision of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school's systems. The office staff are aware of this and control the distribution of these.
- staff are aware that their family members are not permitted to use school devices that may be used out of school
- staff are aware that the use of memory sticks is not permitted.
- 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).

We use CPOMs to record and store sensitive data about pupils which can be accessed on mobile devices using two factor 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.
- All users (adults and pupils) 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 to access each platform they are required to use. The school will keep an up to date record of users.

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.

Learner passwords:

- Usernames and passwords are generated by Mrs Hongkins for each individual learner from Year 1 to Year 6. *These are kept securely should a child forget them and can be reset.*
- Password requirements for learners at Key Stage 2 increases as pupils progress through school.
- Users will be required to change their password if it is compromised.
- Pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important. This is done through Project Evolve and PSHE lessons as well as Internet Safety Day.
-

Technical:

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Our MGL technician has two factor authentication for the admin user account.
- School admin logins are kept in a secure document with MGL. This is only used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
- User resets are carried out by admins and then users can set their own password at the first login.
- *Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by* xxxxx (*insert title*) (schools may wish to have someone other than the school's/college's technical staff carrying out this role e.g. an administrator who is easily accessible to users). *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 xxxxx (insert title) 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 responsible person) *to ensure that the new password can only be passed to the genuine user* (the schools will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a learner)
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use. *(For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, 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:
All users are made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This is also taught as part of our curriculum. All users are taught how passwords can be compromised, so they understand why things should be done a certain way.

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
- staff training on cyber security

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

- in lessons via Project Evolve lessons and PSHE lessons
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:
The responsible person (insert title) 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.

Our filtering service allows us to:

- Change and have flexibility for sites to be added or removed from the filtering list for their organisation
- Remove filtering controls for some internet use (e.g. social networking sites) at for certain users

Responsibilities

The responsibility for the management of the school's filtering policy will be held by MGL. 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 reported to a second responsible person (Mrs Jackson/Mrs Shaw) and then Mrs Jackson or Mrs Shaw will send the request to the MGL helpdesk
- all change requests must be sent to the MGL helpdesk so a record can be kept

All users have a responsibility to report immediately to SLT 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 MGL.
- 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 SLT and MGL. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

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
- 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/newsletters.

Changes to the Filtering System

Changes to the filtering system will be considered by SLT in conjunction with MGL. School must adhere to the following:

- requests should always be sent to the MGL helpdesk
- the grounds on which they may be allowed or denied (schools may choose to allow access to some sites e.g. social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).
- have a second responsible person from MGL be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records/audit of logs)
- ensure we use the MGL helpdesk as an audit/reporting 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 SLT 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 as follows:
Smoothwall filters every user/PC on the network. It flags up any blocks. You can have reports on various aspects of its filtering and at intervals of your choosing.

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

- SLT
- Online Safety Governor (Mr Norris)
- 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-.