Technical Security Policy

(including filtering and passwords)

"Peace be within your walls and security within your towers!"

Psalm 122:7

'Feeding Hearts and Minds'

The peace, joy and love of Christ is at the heart of all that we do in our school. Through religious education, school policy and, primarily, our culture of prayerfulness, charity and joy, we seek to share the Gospel with our families, our parish, our community and the wider world.

Using the example of Jesus Christ, we cultivate the skills of heart and mind that allow us to develop our talents and take a shared responsibility for ourselves, each other and the world He gave us. We profess our faith proudly and recognise that we are called to a loving relationship with God through the sacraments, scripture and prayer.

Our school is animated by love and our shared faith and clear values drive our behaviour and our relationships; we are tolerant and respectful of the unique value of each person. Our individual needs and talents are recognised and nurtured in a warm, inclusive environment where we are able to use our gifts for the glory of God and in loving service of others.

We have excellent role models who empower us to believe in ourselves and provide us with an outstanding education and a wide range of opportunities – our aspirations for the future are high and we believe that through God's grace we can grow, learn and realise our full potential.

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 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 Gill Stables

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
- 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
- Gill Stables 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 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.*
- *remote management tools are used by staff to control workstations and view user's activity*
- *an appropriate system is in place for users to report any actual/potential technical incident to the network manager*

- an agreed policy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school/academy system
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school/academy devices
- the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.

PASSWORD SECURITY

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/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 by Gill Stables who will 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
- 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 students/pupils 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 pupils at Key Stage 2 and above should increase as they 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.

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 school/academy 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.
- *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 Gill Stables. 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.*
- *Requests for password changes should be authenticated 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.
- 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'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
- through the acceptable use agreement

AUDIT/MONITORING/REPORTING/REVIEW:

The responsible person, Gill Stables, 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.

RESPONSIBILITIES

The responsibility for the management of the school's filtering policy will be held by Gill Stables 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
- be reported to and authorised by the Headteacher prior to changes being made

All users have a responsibility to report immediately 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 the Internet Service Provider
- The school has provided enhanced/differentiated user-level filtering through the use of a filtering programme.
- 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 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 the technical staff If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the SLT

EDUCATION/TRAINING/AWARENESS

Pupils 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/newsletter etc.

CHANGES TO THE FILTERING SYSTEM

- Anybody wanting to request changes to the filtering should first apply to Gill Stables who will liaise with the external provider.
- The Headteacher will be involved to provide checks / balances.
- All changes will be logged and reported to the Safeguarding Governor on a termly basis

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 Gill Stables 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.

AUDIT/REPORTING

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

- Online Safety Group
- Online Safety Governor/Governors committee
- FCC Governor 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.

Technical Security Policy

September 2019

The Technical Security Policy is based on best practice advice from Lancashire County Council.

The implementation of this policy will be monitored by Kelly Hannah in consultation with SLT

This policy will be reviewed as appropriate by the FCC committee on behalf of The Governing Body.

Intended Policy Review Date – September 2020

Approved by: _____ (Headteacher)

Date: _____

Approved by: _____ (Governor)

Date:_____