celtic cross education

CCE Technical Security Policy

July 2020

This policy was ratified by the Full Board on Wednesday 15th July 2020. Note that the policy was approved virtually, and signed electronically, due to the circumstances of Covid 19. The policy will be reviewed in July 2021.

Signed: Date: 15th July 2020

Mr P. Wootton, Chair of the Board of Directors

CCE Technical Security Policy

July 2020

Celtic Cross Education Technical Security Policy
July 2020

1. 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 technical network across the trust 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.

2. Responsibilities

The management of technical security will be primarily the responsibility of Celtic Cross Education's chosen external IT provider: TME. Celtic Cross Education's internal IT staff (and staff members from the trust's central office at Unit 15) will support TME to in the management of technical security.

3. Technical Security

3.1 Policy statements

Celtic Cross Education's chosen external IT provider – TME – alongside the trust's internal IT staff, will be responsible for ensuring that the school 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 will receive guidance and training and will be effective in carrying out their responsibilities:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy 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 academy 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.
- TME and Celtic Cross Education's internal IT staff are 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. Where possible, a Mobile Device Management (MDM) solutions should be used.
- TME and Celtic Cross Education's internal IT staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Staff Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity
- Any technical issues with Trust IT equipment should be logged using Parago

  .
- Users should not have the ability to download executable files and install programmes on school devices.
- An agreed policy is in place (Staff Acceptable Usage Agreement) regarding the extent of personal use that staff users and their family members are allowed on school devices that may be used out of school.

- Memory sticks / CDs / DVDs should not be used 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.

Where possible, all mobile devices should be encrypted

User accounts should be deleted by a member of staff at Unit 15 on the day that a user leaves employment of Celtic Cross Education. This staff member must be informed by the academy if an account should be placed on litigation hold.

4. 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).

4.1 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 reviewed incrementally as systems develop and change.
- All academy networks and systems will be protected by secure passwords
- Passwords for new users, and replacement passwords for existing users, will be allocated by a designated staff member from Unit 15 (Rebecca Bishop).
- 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.
- Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below
- The level of security required may vary for staff and student / pupil accounts and the sensitive nature of any data accessed through that account)
- requests for password changes should be authenticated by staff members at Unit 15 to ensure that the new password can only be passed to the genuine user.

4.2 Admin Passwords

- 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
- Where possible, administrative accounts should be protected by two factor authentication.
- Key admin passwords should be unique.
- Device default login credentials should be changed and recorded.

4.3 Staff passwords:

- All staff users will be provided with a username and password by a staff member from Unit 15
- The password 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
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school

4.4. Student / pupil passwords

- All users at KS2 and above will be provided with a username and password
- Passwords will be changed if this becomes necessary.
- Students / pupils will be taught the importance of password security
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.
- Magic badge and Emoji log-in systems may be employed for ease of access for pupils

4.5 Training / Awareness

Members of staff will be made aware of the school's password protocols within this policy:

- at induction
- through the school's Digital Safeguarding Policy
- through the Acceptable Use POlicy

Pupils / students will be made aware of school password policies and related learning:

- in lessons

5. Filtering

5.1 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 trust.

5.2 Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Trust IT Team. They will manage the academy 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 filtering service must

- be logged in change control logs
- be reported to TME / Celtic Cross Education's IT related staff prior to changes being made.

All users have a responsibility to report immediately to the Celtic Cross Education's IT Team 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.

5.3 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 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.

- In all academies, Celtic Cross Education's IT Team 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 the filtering system, allowing different filtering levels for different ages / stages and 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 a nominated senior leader.
- Mobile devices that access the school / academy internet connection (whether school / academy or personal devices) will be subject to the same filtering standards as other devices on the school systems. All devices on the network should be filtered.
- 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 Celtic Cross Education's IT staff / TME and Head of School.

5.4 Education / Training / Awareness

Pupils / students will be made aware of the importance of filtering systems through the online safety education programme (part of the Computing and PSHE curriculums). 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 Staff 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.

5.5 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 Celtic Cross Education's IT Team who will decide whether to make school level changes (as above).

5.6 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.

5.7 Audit / Reporting

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

- SLT / Celtic Cross Education Board / CEO
- External Filtering provider / Local Authority / Police on request

Filtering policies will be reviewed in response to the evidence provided by audit logs of the suitability of the current provision.

6. Backup of Data

6.1. Policy Statements

Data should be backed up on a regular basis.

- Academy servers should be configured with a daily backup regime, backing up to external hard drives which are rotated and stored in a secure location which is not in the vicinity of the server itself.
- Academy servers should also be configured with a full offsite backup.
- Where external and cloud hosting providers are used, a full backup system should be implemented by the provider.