THE BLESSED EDWARD BAMBER CATHOLIC MULTI ACADEMY TRUST

# ICT Security Policy

This is a Trust-Wide Policy which applies to all academies within the Trust

| | |
|---|---|
| **Version:** | **1.0** |
| **Adopted:** | **June 2021** |
| **Next Revision Date:** | **June 2022** |

## 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 academy will be responsible for ensuring that the trust infrastructure 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 trust policies).
- access to personal data is securely controlled in line with the trusts 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 trust computer systems
- there is oversight from senior leaders and these have an impact on policy and practice.

## Responsibilities

The management of technical security will be the responsibility of the Network Manager.

## Policy statements

The academy 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:

- 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 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 academy 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. Details of the access rights available to groups of users will be recorded by the technical team and will be reviewed annually alongside this policy.
- 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.
- the Network 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.
- technical staff regularly monitor and record the activity of users on the academy 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 technical team via the ICT Helpdesk system.
- installation of programmes should be requested via the ICT Helpdesk system and will be accommodated when possible in line with security best practices.

- devices supplied to academy employees should only be used by the employee (e.g. not used as a shared family device).
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on academy devices, all removable devices require encryption, see the trust Data Protection Policy.
- the academy 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 academy site unless safely encrypted or otherwise secured.

## Password/Account Security

A safe and secure username/password system is essential if the above is to be established and will apply to all academy technical systems, including networks, devices, email and online platforms).

## Policy Statements:

- These statements apply to all users.
- All academy networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to academy technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed annually alongside this policy.
- All users (adults and pupils) have responsibility for the security of their username and password, they 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.

## 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 the academy.
- 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 use of a secure password vault solution is also acceptable and recommendations can be obtained from the technical team.

### Learner passwords:

- Records of learner usernames and passwords for foundation phase pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- Password requirements for pupils at Key Stage 2 and above should increase as pupil's progress through the academy.
- 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.
- Under no circumstances should an administrator account be used for any day to day tasks such as web browsing or email access.
- An administrator account password for the academy systems should also be kept in a secure place e.g. academy safe. This account and password should only be used to recover or revoke access.
- 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 the technical. 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.
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use.
- Network accounts are "locked out" following several successive incorrect log-on attempts.
- Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).
- All equipment must have its default credentials changed prior to being put into service, the new password must be tested and verified.
- All staff accounts must be created with standard access, if any member of staff requires any privilege elevation this must be agreed by a member of SLT and the Network Manager, details must be recorded for future reference. All elevated access must be frequently reviewed, amended and recorded as required.

## Training/Awareness:

Members of staff will be made aware of the academy's password policy:

- at induction

Pupils will be made aware of the academy's password policy:

- in lessons

## Audit/Monitoring/Reporting/Review:

The Technical Team 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.

## Responsibilities

The responsibility for the management of the academy filtering policy will be held by the Network Manager. They will manage 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 academy filtering service must:

- be logged on the helpdesk system.
- where a substantial change is requested it must be agreed by a member of the SLT team.

All users have a responsibility to report immediately to the technical or safeguarding team any infringements of the academy 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 academy. Illegal content is filtered by the 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 academy 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 academy network, filtering will be applied that is consistent with academy practice.

- The academy manages its own filtering service.
- The academy has provided enhanced/differentiated user-level filtering through the use of the web 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 member of the SLT.
- Mobile devices that access the academy internet connection (whether academy or personal devices) will be subject to the same filtering standards as other devices on the academy systems.
- Any filtering issues should be reported immediately to the technical team via the ICT Helpdesk.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical team. If the request is agreed, this action will be recorded and logged.

## 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 their class teacher or directly to the technical team who will decide whether to make academy level changes.

## Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The academy will therefore monitor the activities of users on the academy network and on academy equipment as indicated in the acceptable use agreement.

## Audit/Reporting

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

- the SLT team.
- CEO.
- 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.