



THE BLESSED EDWARD BAMBER CATHOLIC MULTI ACADEMY TRUST

ICT Acceptable Usage 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

BEBCMAT maintains certain policies with regard to the use and security of its computer systems, including the network. The below sets out the overview Acceptable Use Policy across the trust but specific pupil and staff expectations can be found in Appendices 1 to 3. Appendixes are to be read in conjunction, and in their entirety, with the overview provided below with all users expected to be familiar with these policies and their content.

Network Security and Privacy Policies

- All users should be aware that the trust monitors and filters internet access. Additionally the trust may also monitor file access, keystrokes and screen images.
- Unauthorised attempts to gain privileged access or access to any account or system not belonging to you on any trust system are not permitted
- Computer and network accounts provide access to personal, confidential data. Therefore, individual accounts cannot be transferred to or used by another individual. Sharing accounts or passwords is not permitted
- Each user is responsible for the proper use of his or her account and any activity conducted within it. This includes choosing safe secure passwords and protecting them accordingly
- No trust system or network may be used as a vehicle to gain unauthorised access to other systems
- Any user who finds a possible security lapse on any trust system or network must report it to the system administrators. To protect your files and the system, don't attempt to use a system under these conditions until a system administrator has investigated the problem
- All users should be aware that the system administrators conduct periodic checks of trust systems and networks, including password checks. Passwords must adhere to the trust password complexity requirements and any user found to have a weak password will be required to choose a secure password during the next login process
- User files on the trust servers are kept as private as possible. Attempts to read another person's protected files will be treated with the utmost seriousness. The system administrators will not override file protections unless necessary in the course of their duties, and will treat the contents of those files as private information at all times

Network and Computing Usage Policies

- No trust system or network may be used for any purpose or in a manner that violates trust regulations or constitutes a legal offence
- Please keep in mind that many people use trust systems and networks for daily work. Obstructing this work by consuming gratuitously large amounts of system resources (disk space, CPU time, print quotas and network bandwidth) or by deliberately crashing the machine(s) will not be tolerated
- Use of any trust system by outside individuals or organisations requires special permission from the Network Manager or technical team
- Use of trust systems or networks for commercial purposes, except where explicitly approved, is strictly prohibited
- Any attempt to vandalise or steal ICT equipment will be treated with the utmost severity
- Users must not attempt to use or install any software not authorised by the trust
- Copying, storing, displaying, or distributing copyrighted material using trust systems or networks without the express permission of the copyright owner, except as otherwise permitted under the copyright law, is prohibited

Portable Device Usage Policies

- Users must obtain permission from a system administrator before connecting any portable equipment to the network
- All laptops connecting to a trust domain must have the managed Anti-Virus client installed and configured to automatically update from the central update server. Any personal devices connecting to the Academy wireless network must have adequate Anti-Virus protection
- Users are permitted to configure their laptops for Internet access at home but are required to frequently connect to the trust network to ensure that they check in with the licence server and relevant updates are applied
- Devices provided to staff are for use by the assigned member of staff only and remain the property of the trust
- All devices provided to staff must be kept securely at all times. The expectation is that when not in use, including when taken home, that devices are locked away securely to prevent theft

Email Usage Policies

- No Email may be sent or forwarded through a trust system or network for an illegal or criminal purpose
- Electronic mail, like user files, is kept as private as possible. Attempts to read another person's electronic mail will be treated with the utmost seriousness. The administrators of email systems will not read mail unless necessary in their duties. Also, there may be inadvertent inspection in the ordinary course of managing and maintaining the computer network and in carrying out other day-to-day activities
- Users should be aware that their "deletion" of electronic information will often not erase such information from the system's storage until it is overwritten with other data and it may, in any case, still reside in the trusts network either on various backup systems or in other forms, and even if erased, may still exist in the form of printouts
- Nuisance E-mail messages or other online messages such as chain letters, obscene, harassing, or other unwelcome messages are prohibited
- Unsolicited emails to multiple users are prohibited
- The trust reserves the right to refuse Email and other connections from outside hosts that send unsolicited, mass or commercial messages, or messages that appear to contain viruses to specific academy or other users, and to filter, refuse or discard such messages.

Limitations of Liability

The trust is NOT responsible for any loss or damage to users' data or disks or for any other problems incurred as a result of using its ICT services, whether the cause originates with the user (for example, misuse of equipment, work left unattended, etc.) or from another source (for example, computer viruses, equipment malfunction, etc.).

Violations of these policies may result in the immediate suspension of computer accounts and network access pending investigation of circumstances and may lead to their eventual revocation. Serious violations of the policy will be referred directly to the appropriate authorities; unauthorised use of trust computing facilities can be a criminal offence. The penalties may be as severe as suspension, dismissal or exclusion for an individual and/or criminal prosecution.

Appendices 1 – Pupil Acceptable Use Policy for Younger Pupils (Primary Academy)

It is clear that complex policies may not be suitable for pupils of a young age. It is important that pupils in a Primary Academy setting are all aware of their requirements as below to ensure they stay safe when using devices:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Appendices 2 – Pupil Acceptable Use Policy for Older Pupils (Secondary Academy)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students/pupils to agree to be responsible users.

For my own personal safety

- I understand that the academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. My passwords will be secure and using best practice with regards to complexity
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the trust systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the trust systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I recognise that the trust has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the trust academies:
- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the trust also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of

school and where they involve my membership of the trust community (examples would be online-bullying, use of images or personal information).

- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could result in loss of access to the trust network, detentions, suspensions, contact with parents and in the event of illegal activities involving the police.

I must ensure when using my personal device for accessing any trust data that:

- The operating system and apps are fully supported by the vendor.
- Any software based firewalls are activated and configured correctly according to best practice
- All devices are receiving regular security updates, which includes updates for any applications
- Recommended password requirements are followed as outlined in the ICT Security Policy
- Anti-Malware/Virus software is installed and kept up to date

Appendices 3 – Staff and Volunteer Acceptable Use Policy (All Academies)

New technologies have become integral to the lives of children and young people in today's society, both within academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that trust systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The trust will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

I understand that I must use trust systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the trust will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school

- I understand that the trust digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the trust.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using trust systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the trusts policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the trust policies
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- The trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:
- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using trust equipment. I will also follow any additional rules set by the trust about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school/academy ICT systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in trust policies
- I will not disable or cause any damage to trust equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the trust Data Policy (or other relevant policy). Where digital personal data is

transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by trust policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for trust sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this acceptable use policy applies not only to my work and use of trust digital technology equipment in school, but also applies to my use of trust systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the trust
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I must ensure when using my personal device for accessing any trust data that:

- The operating system and apps are fully supported by the vendor.
- Any software based firewalls are activated and configured correctly according to best practice
- All devices are receiving regular security updates, which includes updates for any applications
- Recommended password requirements are followed as outlined in the ICT Security Policy
- Anti-Malware/Virus software is installed and kept up to date