Bishop Bewick

Catholic Education Trust

Policy Title:	Acceptable Use Policy for IT Systems
Date of first Approval:	01/11/22
Most recent approval:	23/03/23
Approved by:	Finance & Resources Committee
Date of next review:	Nov 2025

Change log:

Version	Date	Author	Change
1	November 2022	COO	Original
1.1.	November 2023	COO	Minor amends to software references

Acceptable Use Policy for IT Systems

Contents

1. Rationale and Aims

This Acceptable Use Policy for IT Systems is designed to protect the Bishop Bewick Catholic Education Trust, our staff, students and others from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions, both of which should be reported immediately to Senior Team member and the IT support team responsible for IT systems.

The repercussions of misuse of our systems can be severe, for example, loss of student data, or sensitive data being passed on to inappropriate third parties. Potential damage includes but is not limited to: malware infection (e.g. computer viruses); legal and financial penalties for data leakage; and lost learning resulting from network downtime.

Everyone who works for the Bishop Bewick Catholic Education Trust is responsible for the security of our IT systems and the data on them. As such, all staff must ensure they always adhere to the guidelines in this policy. Should anyone be unclear on the policy or how it impacts on their role, they should speak to the senior team member and/or (as appropriate) the network manager responsible for IT systems. A staff Acceptable Use agreement is included as an appendix to this policy. This policy should be read in conjunction with the school's e-Safety policy.

2. Definitions

"Users" are everyone who has access to any of the Bishop Bewick Catholic Education Trust's IT systems (schools, other Trust off-site locations/settings). This includes permanent staff and temporary staff, contractors, agencies, consultants, suppliers, students and business partners, ITT students, governors and visitors.

"Systems" means all IT equipment that connects to school or Trust networks or accesses our applications. This includes equipment owned by the school or personal devices owned by individual members of staff. This includes, but is not limited to: desktop computers; laptops; smartphones; tablets; printers; data and voice networks; networked devices; software; electronically-stored data; portable data storage devices (memory sticks, external hard drives

etc); third party networking services; telephone handsets; video conferencing systems; and all other similar items commonly understood to be covered by this term.

"Sensitive Data" means any personal information of students or staff including but not limited to: name; address; telephone number; date of birth; academic attainment and progress; photographs.

The "Data Protection Act (1998)" controls how personal information is used by organisations, businesses or the government. Everyone responsible for using data has to follow strict rules called 'Data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection.

3. Use of IT Systems

The Bishop Bewick Catholic Education Trust IT systems exist to support and enable learning in our schools. A small amount of personal use is, in most cases, allowed. However, it must not be in any way detrimental to users own or their colleagues work, and nor should it result in any direct costs being borne by the Bishop Bewick Catholic Education Trust. Personal use should be restricted where possible, to before/after school, break or lunchtimes. BBCET trusts its staff to be fair and sensible when judging what constitutes an acceptable level of personal use of the school's IT systems. If staff are uncertain, they should consult their Headteacher or line manager.

Any information that is confidential or sensitive (e.g. contact details of students, PP, LAC information etc) must be encrypted and/or securely stored and/or password protected so that unauthorised access is prevented (or at least made extremely difficult). However, this must be

done in a way that does not prevent–or risk preventing–legitimate access by all properly-authorised parties.

Staff should be aware that any personal documents stored on the school network has the potential to be viewed by monitoring systems. This monitoring must be done to keep us in line with safeguarding requirements. Bishop Bewick Catholic Education Trust can monitor the use of its IT systems and the data on it at any time. This may include examination of the content stored within the email and data files of any user, and examination of the access history of any users.

Bishop Bewick Catholic Education Trust reserves the right to regularly audit networks and systems to ensure compliance with this policy and safeguarding.

4. Data Security

4.1 Sensitive Information

Wherever possible, users should ensure that files which contain personal details of students or staff remain on the school's network (or Office 365) system, and are not transferred to other systems, or stored on personal devices of any kind. This is to ensure the security and integrity of the data and that regular backups are taken, allowing data to be recovered when necessary.

Information stored on portable devices, such as laptops, tablets and smartphones is especially vulnerable. Therefore special care should be exercised with these devices: sensitive information should be stored in encrypted folders only, or password protected. Users will be held responsible for the consequences of the theft, or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it. If sensitive information must be taken out of school on personal devices, it is up to the individual to ensure that the sensitive information is appropriately protected. This information must be deleted/copied back onto the school's IT system at the earliest opportunity.

Users should take great care not to publicly display sensitive information contained in MIS systems etc when using data projectors.

Staff should be cognisant that comments about students which are recorded in a school's reporting/absence tracking software can be viewed by their parents online or requested by parents. All staff, as per the Teachers' Standards, should ensure comments regarding students are appropriate.

4.2 Password Security

Users must keep passwords secure and not allow others to access their accounts. Secure passwords contain a random mixture of lower and uppercase letters, numbers and punctuation. Users will be prompted to change their password on a as per their individual school's practice, but typically not more than 90 days.

4.3 Device Security

Users who are supplied with computer equipment are responsible for the safety and care of that equipment, and the security of software and data stored on it, and on other Bishop Bewick Catholic Education Trust systems that they can access remotely using this device.

All desktops and laptops should be manually locked by the user whenever leaving the machine unattended for short periods, and users must log out when they are leaving the machine unattended for longer periods.

4.4 System Security

BBCET schools have a range of internal and external IT support teams. These teams are responsible for ensuring that the IT systems are properly protected at all times against known threats and vulnerabilities, as far as is reasonably practicable in our school.

However, all users have a duty of care and therefore must, at all times, guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into the Bishop Bewick Catholic Education Trust systems by whatever means. Where incidents do occur, staff must report any actual or suspected malware infection immediately to their Senior Manager and IT support team.

5. Unacceptable Use

All staff should use their professional judgement as to what is unacceptable use of Bishop Bewick Catholic Education Trust systems. However, the activities below are provided as examples of unacceptable use (the list is not exhaustive):

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.

- All activities which are or could be perceived to be detrimental to the success of Bishop Bewick Catholic Education Trust, including defamation of BBCET, the Catholic Church and any of its schools.
- All activities 'for personal benefit only' that have a negative impact on the day-to-day functioning of the school. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).
- All activities that are inappropriate for an Education Trust to be associated with and/or are detrimental to any Trust schools' reputation. This includes pornography, gambling, inciting hate, bullying and harassment. (See your school's e-Safety policy).
- Circumventing the IT security systems and protocols which Bishop Bewick Catholic Education Trust has put in place.
- All personal activities which result in costs being borne by the school or Trust.

Should any member of staff need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their Headteacher before proceeding [For example, pastoral leads/DSL needing to access social media accounts following a pastoral issue].

6. Bring Your Own Device (BYOD)

Bishop Bewick Catholic Education Trust and its schools provide wireless networks which allow staff (sixth form as appropriate) and visitors access to the school's broadband internet service.

Bishop Bewick BYOD service is only for the purposes of work-related activities which need internet access, including:

- any work-related internet activity (school filters operate on all networks)
- email services
- office 365

Staff Acceptable Use Agreement

This Acceptable Use Agreement covers the use of all systems used by Bishop Bewick Catholic Education Trust and its schools as defined in the 'Acceptable Use Policy for IT Systems'.

As a user I confirm that:

- I will only use the IT systems at Bishop Bewick Catholic Education Trust for professional purposes.
- I will ensure that all sensitive data is stored only on systems within Bishop Bewick Catholic Education Trust or Office 365/Google secure cloud storage system.
- I will ensure any personal digital devices used by me do not contain sensitive data relating to students or staff of Bishop Bewick Catholic Education Trust.
- I will ensure any personal devices used in school have adequate antivirus/spyware software installed to prevent infecting school-based equipment via the network.
- I agree that any sensitive data I may need to use for professional purposes while away from Bishop Bewick Catholic Education Trust will be adequately protected using encryption methods and/or password protection.
- I agree to use a secure password to access the IT systems at Bishop Bewick Catholic Education Trust, and to change as per protocol/prompted by my school.
- I will be responsible for the safety and care of any IT equipment loaned to me by Bishop Bewick Catholic Education Trust, and the security of any data stored on it.
- I will lock all desktop / laptop devices while away for short periods
- I will log off all desktop / laptop devices while away for longer periods
- I will take all reasonable steps to ensure any personal digital devices which connect to the IT systems at Bishop Bewick Catholic Education Trust are protected again malware (e.g., viruses, spyware, Trojan horses).

As a user I confirm that I will not: use BBCET's IT systems for the activities stated below:

- All illegal activities, and activities that contravene data protection regulations.
- All activities detrimental to the success of Bishop Bewick Catholic Education Trust as well as defamation of any Trust school.
- All activities for 'personal benefit only' that have a negative impact on the day-to-day functioning of the school.
- All activities that are inappropriate for Bishop Bewick Catholic Education Trust to be associated with and/or are detrimental to the Trusts' reputation.
- Any activity which would circumvent the IT security systems and protocols which Bishop Bewick Catholic Education Trust has put in place.

Employee Name: ……

Employee Signature: ……

School: ……

Date: ……

If there are any issues which would prevent a member of staff from signing this agreement, they must speak to the senior team member responsible for IT systems.