ICT Acceptable Use & E-Safety Policy

(for Staff, Visitors and Volunteers)

For all schools within the Bosco Catholic Education Trust

This policy has been approved and adopted by the Bosco Catholic Education Trust Board.

Approved:	For Review:
July 2023	July 2026

Contents

1. Bosco Catholic Education Trust Mission Statement

The Bosco Catholic Education Trust is a Christ-centred family of Catholic academies, within the Diocese of Arundel and Brighton, working together as one body to provide an outstanding education for all. As Catholic schools, we endeavour to develop confident, compassionate and faithful young people. Through partnership, collaboration, and mutual support, we seek to enable all those entrusted to our care to become the person God called them to be.

"Serve the Lord joyfully"

2. Introduction

The Trust is dependent on *Information Communication Technology* (ICT) to deliver learning, teaching, and day-to-day operations. The proper, secure, and appropriate use of ICT is vital to maintaining a robust infrastructure, and safe nurturing environment where all can work, learn, and thrive.

This policy describes the acceptable use of ICT that will protect the interests of our users and the Trust/schools, so that:

- ICT-use complies with legal requirements.
- The maximum benefit is obtained from our investment in ICT facilities.
- Risks arising from improper use of information, identity or equipment are minimised.
- Individual users have confidence that they can only be held accountable for their own actions and not those of others.

The responsibility for careful, diligent, and considerate technological and data handling practice and e-safety awareness rests with all who work with young people, paid or unpaid.

As a condition of the Trust's insurance policy, all employees and governors must undertake the National Cyber Security Centre's (NCSC) training annually and complete a register to evidence this. The necessary training can be found on *My Bosco* and will be disseminated by IT Services annually.

If you are ever in doubt about doing the right thing, or should you require any further support with this policy, please do not hesitate to contact IT Services by calling **01444 221779**, or by email using **ITservices@boscocet.org.uk**.

It is the responsibility of the user to take all reasonable steps to ensure compliance with the conditions set out in this policy, and to ensure that misuse of ICT systems does not occur.

3. Your Work Account

To protect your work account and identity:

- You must not impersonate any person or misrepresent your identity including using another person's username, password, or other account information.
- Do not reveal your password to anyone. If you think an unauthorised person knows your password, then contact IT Services immediately.
- You should notify IT Services immediately of any unauthorised use of your username, password, other account information, or any other breach of security that you become aware of.
- Do not reveal any personal information (e.g., home address, telephone number) about yourself or other users.
- Do not trespass into other users' files or folders and never use another user's account for any purpose.

- Lock your computer or log out whenever you are leaving it unattended.
- If using an iPad, ensure your device is protected by a passcode to prevent unauthorised access. If using another device, ensure that it is 'locked' when you are away from it.

4. Internet Access and Filtering

The internet is an invaluable resource for learning, teaching, and day-to-day operations. A safe, filtered internet connection is provided by the school for this purpose.

- Internet access provided by the Trust/school is not private. The Trust/school monitors and filters internet usage to improve delivery of service and to safeguard its community of users.
- Any access to the internet from the Trust/school's network can be traced to the Trust/school. You must not use the internet in any way that might bring the Trust/school into disrepute.
- Incidental personal use of the internet is permitted if usage is limited to a reasonable amount and does not interfere with your work.
- If, as part of your incidental personal use of the internet you are required to provide an email address, you should use a personal email and not use your work email address.
- If your line manager is concerned that you are making excessive private use of the Trust/school's internet or accessing inappropriate sites, they can take disciplinary action.
- Use of the Trust/school's internet for personal financial gain, gambling, political purposes, or advertising is forbidden.
- Attempting to access or accessing pornography, exploitative, offensive, discriminatory, violent, racist, harmful, or criminal content is forbidden. You should inform IT Services immediately if you inadvertently access any such material.
- Action will be taken if you are attempting to access inappropriate sites, or if you are using the internet excessively. If the activity is illegal, the authorities will be informed.
- When using materials from the internet, you must respect the author's copyright.
- If downloading files from the internet, you must exercise extreme caution to ensure the source is trustworthy and malware-free.
- Some users are granted access to VPN to connect to work systems remotely via a secure connection. You must not share VPN credentials with any other user. You are not permitted to use VPNs when at work.

5. Emails & Online Communication

You are responsible for the emails and chat/conversations that you send. Be polite, respectful, and professional always and think carefully about the language you use.

- Email and other online communication methods such as Teams are owned by the Trust/school. These communication methods are not private and are monitored by the school.
- You must limit use of incidental personal email to ensure that it does not interfere with your work. If your line manager is concerned about excessive use of email, they may take disciplinary action.
- You must use your work-provided email address(es) for all work-related purposes.
- If you are required to provide an email address for non-school related sites or services, you should provide a personal email and not use your work email address.

- Do not use language that is:
    - defamatory, abusive, harassing, threatening, or an invasion of privacy of another person.
    - bigoted, hateful, racially or otherwise offensive.
    - violent, vulgar, obscene, pornographic, or otherwise sexually explicit.
    - otherwise harmful, or can reasonably be expected to harm, any person or entity.
- Always be professional and respectful; do not infringe on the rights or privacy of others, or make ill-considered comments or judgments.
- The school may block email that is deemed to be inappropriate.
- Protect your personal identify by not revealing personal details of yourself or others in emails or online communications, such as address or telephone number. Exercise caution if arranging to meet anyone you do not know.
- Question the authenticity of all emails but especially those received from email addresses that do not belong to a Trust school.
- Do not share images of other students or staff without the express permission of all involved.
- Posting anonymous messages and forwarding chain letters is forbidden. Users must declare who they are in all online communication.
- You must not use email or other online communication if the activity:
    - is illegal, or encourages or advocates illegal activity, or the discussion of illegal activities with the intent to commit them. This includes messages relating to child pornography, stalking, sexual assault, fraud, trafficking in obscene or stolen material, drug dealing and/or drug abuse, harassment, theft, or conspiracy to commit any criminal activity.
    - infringes or violates any right of a third party including: (a) copyright, patent, trademark, trade secret or other proprietary or contractual rights; (b) right of privacy; or (c) any confidentiality obligation.
    - is commercial, business-related or advertises or offers to sell any products, services or otherwise.
    - is sending spam or other unsolicited commercial email or sending information that is fraudulent or is not transparent as to its source, such as “spoofing” or “phishing”.
- If you receive an email that contains material that you feel is offensive, discriminatory, or criminal, you should report this immediately to your line manager or IT Services.
- Writing or forwarding emails or messages that contain pornographic, exploitative, offensive, discriminatory, or criminal content will result in disciplinary action. If the content is illegal, the police will be informed.

6. Social Media

The Trust/school respects privacy and understands that staff and learners may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the Trust/school’s reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a Trust/school account, or using the Trust/school name. Professional communications are within the scope of this policy. Personal communications are those made via a personal social media account. Where a personal account is used which associates itself with, or impacts on, the Trust/school, these personal communications fall within the scope of this policy. Personal communications which do not refer to or impact upon the Trust/school are outside the scope of this policy.

- Staff may use social media to communicate with learners via a Trust/school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.
- School accounts must be monitored regularly and frequently.
- Social media communications must adhere to the standards set out in this policy (especially section *3 Email & Online Communications*) and other relevant policies.
- Trust/school social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the Trust/school.
- If a journalist makes contact about posts made using social media, staff must report this to the school's headteacher, or the CEO/CFO of the Trust before responding.
- When acting on behalf of the school, respond to harmful and/or offensive comments swiftly and with sensitivity. If a conversation becomes offensive or unacceptable, block, report or delete other users or their comments/posts swiftly.
- The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing online content are engaging, conversational, informative, and professional.
- Staff are not permitted to follow or engage with current or prior learners of the school on any personal social media account.
- The Trust/school's education programme should enable learners to be safe and responsible users of social media. Learners are encouraged to comment or post appropriately about the Trust/school. Any offensive or inappropriate comments will be resolved using the Trust/school's behaviour policy.
- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The Trust/school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/carers are encouraged to comment or post appropriately about the Trust/school. In the event of any offensive or inappropriate comments being made, the Trust/school will ask the parent/carer to remove the post and will invite them to discuss the issues in person or follow the Trust/school's complaints procedure.

7. Using the Network & Cloud Storage

- You must use your own login credentials to access local and cloud network storage.
- Networked resources and cloud storage are intended for educational purposes and may only be used for legal activities consistent with the rules of the Trust/school. You must use the services and resources for the purposes for which they are made available.
- Any use of the network that would bring the name of the Trust/school into disrepute is not allowed.
- Do not use the network in any way that would disrupt use of the network by others.
- Users will accept personal responsibility for reporting any misuse of the network or security loopholes to IT Services immediately. You must not demonstrate the problem to other users.
- Files held on the Trust/school's network and in cloud storage are monitored by the Trust/school.
- You must not save program files (.exe files) or other potentially harmful filetypes on the network.

- Do not save pictures, music, or video files unless you have created them yourself. Doing so takes up unnecessary space and may break the author's copyright. Copyright of materials must be respected.
- Files stored in network locations will be checked regularly and deleted without warning if deemed unsuitable.
- You should store work in OneDrive to ensure it is appropriately backed up and is accessible from any device. If you have a school-provided iPad, you should ensure the device is configured to back up to iCloud to ensure your apps and photos are also backed up.
- You should not use any other cloud storage alternatives other than those provided by Trust/school.
- You must not install software on the Trust/school's network or make any changes to network, system, or service configuration settings.
- You are not permitted to connect any equipment to the network without prior agreement and approval by IT Services.
- You must not reconfigure the network in any way, including enabling peer-to-peer capabilities, file sharing, or remote access.
- Users identified as a security risk will be denied access to the network.

8. Generative Artificial Intelligence

When used appropriately, generative Artificial Intelligence (AI) has the potential to reduce workload, free up teachers' time and create exciting new learning opportunities for learners.

- Never enter personal or sensitive data into generative AI tools to protect data privacy. Generative AI stores and learns from inputted data, and therefore the data should not be identifiable. Once data is provided to AI, it should be considered public information.
- Generated content can be inaccurate, unreliable, or unsubstantiated, and therefore content requires academic scrutiny and professional judgement to assess appropriateness and accuracy.
- Generative artificial intelligence returns results based on the data it has been trained on. It is unlikely to have been trained on the curriculum specifically as you teach it. You should not assume that generated content will be comparable to human-designed resources that have been developed in the context of the curriculum.
- If AI is used to assist with the creation of administrative plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produces it and the organisation they belong to. All laws relating to copyright and attribution must be adhered to.
- Schools may wish to review homework policies to consider the approach to homework and other forms of unsupervised study as necessary to account for the availability of generative AI.
- Generative AI has enormous potential for learning, but to harness this potential, students need to be knowledgeable and develop their intellectual capability:
    - Even though generative AI can produce fluent and convincing responses, the content can be factually inaccurate. Foundational knowledge and skills become essential in discerning the accuracy and appropriateness of information, so a knowledge-rich curriculum is even more important.
    - Education has a duty to prepare students for changing workplaces, including teaching them how to adapt to emergent technologies safely and appropriately. At appropriate milestones, this should include understanding the limitations, reliability, and potential bias of generative AI, including how information on the internet is organised and ranked, and what constitutes harmful or misleading content. Learners should receive regular age-appropriate education in how to protect themselves from harm in online contexts.

- Schools need to continue to take reasonable steps, including complying with guidance from the Joint Council of Qualifications and examining bodies, to prevent malpractice, including malpractice involving use of generative AI. There are already strict rules in place, set by exam boards, to ensure pupils' work is their own.
- Generative AI can generate convincing content of all kinds including that which is potentially harmful, for example, highly credible scam emails requesting payment that are more authoritative and believable than seen previously. It is more important than ever that users are informed in cyber threats and can apply professional judgment to manage risk.
- Appropriate filtering and monitoring standards should be in place to prevent children and young people from accessing or creating harmful content through generative AI.

Adapted from the Department of Education's departmental statement on *Generative Artificial Intelligence in Education* (2023).

9. Harmful & Illegal Activity

Access to systems and data are provided to you for the purposes of learning, teaching, and day-to-day operations.

- You may only access information on Trust/school systems if you have been properly authorised to do so and if you need the information to carry out your work.
- Unauthorised access to or modification of data is a criminal offence under the Computers' Misuse Act 1990.
- Illegal activities of any kind are strictly forbidden. Any illegal activities will be reported to the authorities.
- It is illegal to circumvent any access or authentication restrictions, or otherwise attempt to compromise the security of the Trust/school's systems.
- You must not probe, scan, or test the vulnerability of any part of the Trust/school's systems without proper authorisation.
- Activity that threatens the safety of the Trust/school's ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- If a virus is detected, you must report this to IT Services immediately.

10. Physical Security & Damage

- Users are expected to exercise good handling and care of all work-provided hardware and to maintain sound physical security of hardware they are using.
- All work-provided hardware is recorded in the Trust's asset management system and must not be moved from its location without notifying IT Services first. If you move equipment yourself, this may invalidate any warranty.
- You must ensure computers and tablets are locked or signed out when left unattended to prevent posing a significant risk to the security of data and information. If you are leaving a device for a longer period, please turn the device off to minimise any security risk further.
- You must be careful to prevent work-provided equipment from being lost or stolen.
- Any malicious attempt to harm or destroy any equipment or data will result in loss of access, disciplinary action such as exclusion and, if appropriate, legal referral.
- The use of software from unauthorised sources is prohibited.

- Memory sticks and other portable devices should never be used to transfer data to or from Trust/school. You should use OneDrive where possible to save data to the cloud instead. If you need to transfer data via another method, for example, for exam board moderation, please contact IT Services for an exemption.
- When your employment ends, you must return all work-owned equipment to IT Services immediately. IT Services will ensure devices are erased.
- When equipment reaches the end of its useable life, IT Services will dispose of the equipment in accordance with WEEE regulations.

11. Use of Hardware & Personal Devices

- You may connect a personal mobile device to the Trust/school's Wi-Fi network for your convenience, but please note this *Acceptable Use Policy* applies to all devices where you use Trust/school systems or services including on your personal mobile.
- Other personal devices (except for mobile phones) are not permitted on our sites unless explicit permission has been granted by IT Services.
- Where IT Services grant permission for the use of a personal device for work purposes, for example, a laptop or tablet, the device will not be given full network access, but instead will have limited access to resources and the internet.
- The Trust and its schools are not responsible for damage, loss, or theft of personal devices. Personal devices are brought onto Trust/school sites entirely at the risk of the owner. It is the owner's responsibility to ensure the device is insured appropriately when out of the home.
- Passwords or passcodes should be set up on the device to aid security.
- It is the owner's responsibility to ensure the device is updated with the latest security updates and patches. Devices must be free of viruses and malware and have appropriate software to detect potential threats. It is the owner's responsibility to check with IT Services if they are unsure.
- All devices are subject to routine monitoring.
- Staff-owned devices, including mobile phones, should not be used for personal purposes during lessons, and use should be kept to a minimum during work hours. Exceptional circumstances should be agreed with the user's line manager or a senior member of staff.

12. Use of Software

- Software is provided to you to carry out your day-to-day workload and to deliver Trust/school services.
- Only software properly purchased and/or approved by IT Services may be used on school computer systems. You may not install software acquired through other means on to any Trust/school owned assets, including desktop computers, laptops, tablets, or mobiles.
- You may not use any software service delivered 'down the wire' (e.g., Google Documents) for any work-related activity unless provided by IT Services. Such solutions may store information in locations where data protection and unauthorised access is neither illegal nor uncommon.
- The use of, or copying, software without the licensor's permission is illegal and the terms and conditions of software licenses must always be adhered to. Any person carrying out illegal software copying is legally liable and may be prosecuted.
- Changes may not be made to the configuration of software except by IT Services or someone authorised by them to make the changes.

- Whilst it is your responsibility not to deliberately change the configuration of your computer software, it is possible for software to be installed on a machine without the full knowledge of the user. If you discover software that has been installed in an unsolicited manner, contact IT Services who will be happy to assist in resolving any issues.
- If your needs cannot be met by the software solutions provided to you, please discuss the matter with your line manager or IT Services.

13. Photography

- If photographing others, for example, on trips/visits, events, performances, and in other activities, please respect individual's preferences and do so with their permission.
- Written permission from the parent/carer should be obtained before photographs of students are published (for example, on the Trust/school's social media or websites). This permission is usually requested when the child joins the school and is held on file but can be modified by the parent/carer at any time.
- Named images of students will only be published beyond the school's media, for example, in TV presentations, newspapers, websites outside of the Trust etc, when separate written consent is obtained from the parent/carer.
- Under no circumstances should staff share or upload learner pictures online other than via official Trust/school channels.
- Staff should exercise their professional judgement about whether an image is appropriate to share on Trust/school social media accounts. Learners should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

14. Data Handling & Care

- Your work should be stored in OneDrive to ensure that it is backed up appropriately.
- Do not share sensitive data or information via email. Instead, share information via OneDrive using your email so that access can be revoked if necessary. IT Services can support you with this.
- In accordance with the Freedom of Information Act, all information should be made available on request unless covered by exemptions such as personal data, which is covered by the Data Protection Act & GDPR.
- You are trusted to act responsibly with personal data, and it must only be used to help you to carry out your job. It must not be passed directly, or indirectly through neglect, to people who have no right to see it.
- Unauthorised release of personal information is likely to be treated as misconduct under our disciplinary procedures. You could also be held legally liable for actions that break the Data Protection Act & GDPR, such as failing to ensure the confidentiality of data.
- Data and information that is used to deliver services should be held on corporate systems in line with our Acceptable Use Policy and as directed by IT Services. This means that databases held on single PCs, usually Microsoft Access databases, should not be used for service delivery. IT Services can advise on an appropriate solution.
- The Trust's OneDrive cloud storage may be used to share data between multiple devices both within and outside of the Trust/school's network. Usage is limited to departmental resources for teaching and learning

and cloud services should not be used for storing confidential information, student details or photographs of students.

- Data and information should only be kept for as long as they are needed for legal, operational, or other business reasons. For support with this, please contact the Trust/school's Data Protection Officer.

15. Use of Voice Services

- Voice services and equipment are provided to you to support your day-to-day workload and the delivery of Trust/school services.
- Calls may be monitored and recorded without warning.
- Incidental telephone use for private calls without charge is permitted if it is limited to a reasonable amount. Such use must not interfere with work responsibilities.
- If your line manager is concerned that you are making excessive private use of the telephone system, they can take disciplinary action.
- Internet, telephone calls or email access via personal mobiles are still subject to this Acceptable Use Policy.
- If you lose your mobile phone and you are signed into work email, telephony, or any other work-provided service, please contact IT Services immediately for assistance.
- Do not make or answer calls whilst driving unless using the appropriate hands-free technology.
- Do not allow anyone else to use your mobile phone.
- Access to email, telephony or any other work-provided service must be removed from your mobile when you leave your job.

16. Consequences of Misuse

This policy applies to employees on permanent, temporary, and fixed-term contracts, temporary or casual staff, volunteers, contractors, and other staff employed by a third-party who use our facilities.

- Any breach of these conditions may lead to withdrawal of the user's access, disciplinary action, or termination of contract.
- In the case of illegal activities, the matter will be referred to the relevant authorities and may result in criminal prosecution.
- Staff are expected to comply with the terms set out in other documents relating to their role or function such as the Trust/school's HR manual.
- All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

17. Password Policy

All users must adhere to the following password policy for all accounts used in conjunction with the Trust/school:

- **The minimum length of a password is 14 characters.** We recommend a combination of unrelated words (known as a passphrase) which can be comprised of upper (A-Z) and lower (a-z) case, digits (0-9) and special characters for maximum strength (see below for examples).

- **There is no limit to the maximum length of a password**. We encourage you to adopt passphrases that are naturally more secure and easier to remember since they do not involve random numbers and special characters.

- **Special characters can make a password much stronger** but choose how you use them carefully as they can make passwords difficult to remember. The following special characters are supported: (~! @#$%^&*()+=_-{}[]\|:;"?/<>,.')

- **You may use the same password to log onto:**

  a. **Your Work-Provided Device(s)**
  b. **Office 365**

  However, you must not use this same password for any other service irrespective of whether this service is for work use or personal use.

- **You should use different passwords for each service outside of those listed above**.

- **You may allow the browser to store/remember passwords for ease of use**. Password managers are also permitted, however, please discuss this with IT Services to ensure the manager you are using is safe and secure.

- **Never share your password with anyone.** This includes IT Services. Never communicate passwords via email, telephone, Teams chat or any other means. Passwords should never be written down.

- **When setting up password 'hints', do not hint at the format of your password** (for example, *"Middle Name + Birthday"*.

- **You will not be required to frequently refresh your password** providing that it meets all the above criteria. If your password does not meet some or all the criteria above, please change your password immediately.

- **All accounts must be protected by multi-factor authentication where the option for this exists.**

18. Bibliography

Department for Education (2023) *Generative Artificial Intelligence in Education*. available here.