ICT and Internet Acceptable Use

St Benedict
CATHOLIC ACADEMY TRUST

Authors:	Digital Strategic Leader
Effective Date:	01 September 2025
Last Review Date:	October 2025
Review Frequency:	Annually
Next Review Due:	Autumn 2026

ST BENEDICT CATHOLIC ACADEMY TRUST

ICT AND INTERNET ACCEPTABLE USE

Our mission is inspired by our Patron St Benedict, to live, learn, pray and celebrate together. Our community of Catholic schools are committed to ensuring that each child realises their God given gifts. Our strong sense of community promotes Gospel values which inspire students to make a positive contribution to society. We provide the best possible opportunities for every child's education, with an overarching mission focused on delivering a strong Catholic education, firmly rooted in the belief that Christ should be at the core of all our endeavour.

Contents

Introduction and aims

Information and communications technology (ICT) is an integral part of the way the St. Benedict Catholic Academy Trust and schoolwork. ICT and the internet are a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of Trust and school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use
- This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
    - Breaches of this policy may be dealt with under our Behaviour and inclusion policy/ staff code of conduct.

Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- DfE Policy Paper: "Generative artificial intelligence (AI) in education" (June 2025)
- Data Protection Act 2018 - Data Protection Act 2018
- The General Data Protection Regulation (GDPR) - General Data Protection Regulation (GDPR)
- Computer Misuse Act 1990 - Computer Misuse Act 1990
- Human Rights Act 1998 - Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 - Regulation of Investigatory Powers Act 2000
- Education Act 2011 - Education Act 2011
- Freedom of Information Act 2000 - Freedom of Information Act 2000
- The Education and Inspections Act 2006 - The Education and Inspections Act 2006
- Keeping Children Safe in Education 2025 - Keeping Children Safe in Education
- Searching, screening and confiscation: advice for schools - Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC) - National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021
- Online Safety Act 2023
- DfE Filtering and monitoring standards & DfE Cyber security standards
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Definitions

- **"ICT facilities"**: includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

- **"Users"**: anyone authorised by the Trust or school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

- **"Personal use"**: any use or activity not directly related to the users' employment, study or purpose

- **"Authorised personnel"**: employees authorised by the Trust or school to perform systems administration and/or monitoring of the ICT facilities

- **"Materials"**: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix for a glossary of cyber security terminology.

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way
- Creation and sharing of misinformation, disinformation and conspiracy theories.

This is not an exhaustive list. The school reserves the right to amend this list at any time.

The Trust, Principle/ Headteacher and Senior Leadership team or any other relevant member of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Exceptions from unacceptable use

Where the use of Trust or school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Trust or Principal's discretion.

Please email the Trust digital lead, Principal/ Headteacher or IT manager with the proposed use and a decision will be made.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour and the staff code of conduct.

- Behaviour & Inclusion Policy
- Staff code of conduct

Use of Ai in School

For more information, please refer to - Use of AI

Staff (including governors, volunteers, and contractors)

Access to Trust and school ICT facilities and materials

The Trust and school's IT manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones, Chromebooks and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the Trust and school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT manager.

If a member of staff does not have permission to files or facilities that they require please contact the IT and a decision regarding your request will be made.

Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the IT manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

For more information regarding Mobile use and email communication See Mobile phone Policy and Communications channels guidance.

Personal use

Staff are permitted to occasionally use Trust or school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Principle/ IT manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the Trust or school's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the Trust or school's ICT facilities for personal use may put personal communications within the scope of the ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the Trust or school's Mobile phones policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (See social media policy). Staff should use the information in this policy to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is always appropriate. The recommend that Social Media accounts are set to private where possible.

(See Social Media Policy.)

Remote access

Teachers are provided with the capability to remotely access files through either Microsoft or Google accounts for educational purposes. It is imperative that when utilising these accounts outside of the school environment, both staff and students strictly adhere to the acceptable use policy set forth by the Trust and school IT Department.

This includes but is not limited to exercising caution in sharing sensitive information, maintaining confidentiality, and refraining from engaging in any activities that may compromise the security or integrity of the IT systems.

In order to access Microsoft 365 services 2Fa has been enabled when accessing accounts outside of the school network. Adapt to reflect if school has 2fa.

School social media accounts

Adapt this sub-section to reflect your school's approach.
The school has two official Twitter pages. One for the main school and one for Careers, managed by Admin staff and the Digital Strategic Leader. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they always abide by these guidelines.

(See Social Media Policy.)

Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications
- Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Pupils

Access to ICT facilities

- "Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff"
- "Specialist ICT equipment, such as that used for Computer Science & IT, Music, Design and Technology and Media Studies must only be used under the supervision of staff".

Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

- See Mobile Phone Policy
- See Online Safety Policy

Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour and inclusion policy, if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting, cyberflashing or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Sanctions for unacceptable use of IT

Unacceptable IT use is deemed a serious or very serious incident and the procedures outlined in the behaviour policy will be followed.

Parents

Adapt this sub-section to reflect your school's approach.

Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course. Parents can request access to some school-based IT systems for example Google Classroom Guardian and Bedrock. This will allow the parent to receive updates of classroom assignments and set tasks.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the school's facilities at the Principal/ Headteacher discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the school online

We believe it is important to model for pupils, and help them learn how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

- See Social Media Policy

Data security

The school is committed to ensuring the security of its computing resources, data, and user accounts. Our approach to cyber security aligns with the standards and recommendations set out in the DfE's "Meeting digital and technology standards in schools and colleges" and the National Cyber Security Centre (NCSC).

All users must adhere to safe computing practices. Breaches of the following security protocols may result in disciplinary action.

- See Data Protection Policy

Governance and Risk Management

- The Trust and school's will conduct a cyber security risk assessment at least annually to identify, evaluate, and mitigate risks to our systems and data.
- The governing board, in conjunction with the Trust, Principal/ Headteacher, Digital Lead, and ICT Manager, holds ultimate responsibility for the school's cyber security strategy and its implementation.
- Our business continuity and disaster recovery plan include a specific, regularly tested contingency plan for responding to a cyber security incident, such as a data breach or ransomware attack.

Access Control

- User Accounts: All users will be provided with a unique user account. Users are responsible for all activity on their accounts.

- Principle of Least Privilege: User accounts will be granted access only to the information and systems required for their role. The ICT Manager will conduct regular reviews of user access privileges to ensure they remain appropriate.
- Passwords: Passwords must be strong and not easily guessable. They must not be shared with any other person.
- Multi-Factor Authentication (MFA): Where available, MFA (also known as 2-Factor Authentication or 2FA) must be enabled on all accounts, especially those accessing personal or sensitive data (such as email and the Management Information System). This provides a critical additional layer of security.
- Logging Off: Users must log out of systems and lock their devices when not in use to prevent unauthorised access.

Technical Defences

- Firewalls and Filtering: The school network is protected by a firewall and content filtering systems. These systems are regularly reviewed and updated to ensure they remain effective against current threats and meet the DfE's filtering and monitoring standards.
- Anti-malware: All school-owned devices must be protected with up-to-date anti-malware software.
- Software and Patching: All software and operating systems must be licensed and kept up to date with the latest security patches. Users must not attempt to circumvent or disable automatic updates.
- Personal Devices: Any personal device connected to the school network must have up-to-date anti-malware software and operating system security updates installed.

Data Protection and Encryption

- All personal data must be processed and stored in line with the UK GDPR, the Data Protection Act 2018, and the school's Data Protection Policy.
- Sensitive or confidential data must be encrypted when stored on portable devices (e.g., laptops, USB drives) or sent via email.
- Staff must not enter any personal or sensitive data about pupils or staff into public web services or applications, including public Generative AI tools, without explicit authorisation from the Data Protection Officer.
- Any suspected data breach must be reported immediately to the Trust, ICT Manager or school's Data Protection Officer in line with our data breach procedure.

See Data Protection Policy

Training and Awareness

- The school will provide mandatory cyber security training for all staff at induction and at least annually thereafter.
- Training will cover key security risks, including how to identify and report phishing emails, the dangers of social engineering, password security, and the safe use of school systems and data.
- The curriculum will provide opportunities for pupils to learn about online harms and develop their digital literacy and critical thinking skills to stay safe online.

Incident Response

- The Trust or school has a cyber incident response plan to ensure we can respond effectively to any security breach.
- Backups: Critical school data is backed up regularly. These backups are stored securely in a separate location and cloud-based, and restoration is tested regularly to ensure data can be recovered in an emergency.
- Ransomware: The school will not engage with criminals or pay ransoms in the event of a ransomware attack. We will instead rely on our tested backups and incident response plan.

Please see the glossary (appendix 2) to help you understand cyber security terminology.

Protection from cyber attacks

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Provide opportunities for students to learn about online harms, including misinformation and disinformation, to develop their digital literacy and critical thinking skills.
- Put controls in place that are:
    - 'Proportionate': the school will verify this using a third-party audit annually, to objectively test that what it has in place is up to scratch
    - Multi-layered: everyone will be clear on what to look out for to keep our systems safe
    - Up to date: with a system in place to monitor when the school needs to update its software

- Regularly reviewed and tested: to make sure the systems are as up to scratch and secure as they can be. This includes the filtering and monitoring standards for schools set out by the DfE.

Internet access

The school wireless internet connection is secured and is filtered using web monitor software, internal Firewall and antivirus protection, and a Firewall.

Staff and Student web activity is monitored. If a member of staff suspects that a student has been misusing internet services, they must alert and report to the Trust IT manager or school IT department.

The Trust IT manager or school IT department can provide members of staff with internet access reports and routinely monitor web activity. In the event of misuse, the IT department updates the filters to ensure that staff and students cannot gain access to inappropriate websites.

The filters are not fool proof but there is a continued commitment by the IT department to ensure that filters are as secure as can be while providing the best experience for staff and students using the network.

Student

Adapt this sub-section to reflect your school's approach.
Only applicable if students have access to a school-based device.

Students can access the WiFi network to connect a school-based device to be used for educational purposes online. Students must follow the ICT and internet acceptable use outline in this policy.

Parents and visitors

Parents and visitors to the Trust or school will not be permitted to use the WiFi unless specific authorisation is granted by the Principal/ Headteacher or IT Manager.

The Principal/ IT Manager will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's WiFi to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Governors may need to request access to connect their devices during governors' meetings.

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Monitoring and review

The Trust, Principal/ Headteacher, Digital Lead and ICT manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Trust and schools.

This policy will be reviewed annually.

The governing board is responsible for approving this policy.

Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour and inclusion
- Staff code of conduct
- Data protection
- Remote learning
- Mobile phone
- Social Media
- Generative Ai

Appendix 2: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.

TERM	DEFINITION
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.