Acceptable Use Policy

Policy owner	Trust Inclusion Lead
Policy approved by	Finance, Audit & Risk Committee
Policy approved	
Review frequency	2 years
Policy next approved	

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our Trust works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

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

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur 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 staff code of conduct/disciplinary policies.

This policy will be reviewed annually and should be read alongside our Child Protection and Safeguarding Policy.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021

- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Responsibilities

All staff at St Barnabas Multi Academy Trust (MAT) must be aware of the following responsibilities both at work and off-site:

- All staff understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops, smart devices (watches etc.) and tablets.
- All staff understand that it is a disciplinary offence to use the school ICT equipment for any purpose not permitted by its owner.
- No staff will disclose any passwords provided to them by the school to anyone.
- All staff understand that they are responsible for all activity carried out under their username.
- Staff will not install any hardware or software on any school owned device without the Head's permission, who should seek approval from the CEO.
- Staff will not use any school device for personal use or store any personal data on said devices.
- All staff understand that their use of the internet may be monitored and if anything that breaches unacceptable use is uncovered (as below), it could be logged and used in line with any disciplinary procedures. This includes all school owned devices. If an E-safety incident should occur, staff will report it on Safeguard my School in line with safeguarding training as soon as possible.
- All staff are required to report a security incident/personal data breach as soon as it is detected to the Head of School who will escalate it (if required) to the IT Support/Data Protection Officer.

4. Access to school ICT facilities and materials

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

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

5. Unacceptable Use

The following is considered unacceptable use of the Trust's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings

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
- 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 programme, tool or item of software designed to interfere with the functioning of the school's 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 the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel 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 or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Continuing to use an item of software or hardware after the St Barnabas MAT or its authorised IT representative has requested that use cease because it is causing disruption to the correct functioning of the network
- Other misuse of the network, such as the introduction of "viruses" or other harmful software to resources on the network, or on another User Organisation's network.

No passwords should be divulged, no memory sticks should be used and no sensitive data (as covered by GDPR and safeguarding training) should be removed from site unencrypted, the only approved method of information being retrieved off site is through Google Workspace (this includes Google Drive) unless there is explicit confirmation of alternative means from the MAT Board.

Personal devices must only be used in the context of school business, in line with GDPR and with the explicit permission of the Head who should seek approval from the CEO. Personal mobile phones, smart devices (watches etc.) or digital cameras must NEVER be used for taking any photographs related to school business. Each class has a device specifically for this purpose. These school devices must NEVER be used for personal use.

Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. Parental consent is recorded in line with GDPR for their children's images being used in our brochure or in the local press. If a parent does not agree to this, we ensure that their child's photograph is not used. When possible, a professional photographer will come to school to take photographs of children. These will then be made available to parents.

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Head Teacher/CEO/authorised IT representative will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities**.**

6. Passwords

All users of St Barnabas MAT ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

All staff will use the password manager required by the IT manager to help them store their passwords securely.

7. Software updates, firewalls and anti-virus software

All St Barnabas MAT ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the MAT's ICT facilities.

8. Use of phones and email

The school provides each member of staff with a St Barnabas 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/carers 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 Head of School/I.T Manager immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers 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.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

WhatsApp is a non sanctioned platform for official school business. With the DfE 2030 digital standards, schools are expected to move internal communication to platforms like Google chat which have audit trails.

9. Personal use

Staff may not use the 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 school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

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/carers could see them.

Staff should take care to follow the school's guidelines on use of social media to protect themselves online and avoid compromising their professional integrity.

10. Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

11. School social media accounts

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 may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

12. Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. St Barnabas Trust uses Securely to filter and monitor online use.

The school monitors ICT use in order 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

Our governing board is responsible for making sure that:

The school meets the DfE's filtering and monitoring standards

- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
- For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems
- The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

- Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

13. Data security

St Barnabas MAT is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

14. Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy which can be found on the MAT website or requested from the DSL.

15. Clear Desk and Clear Screen Policy

- In order to reduce the risk of unauthorised access or loss of information, St Barnabas MAT enforces a clear desk and screen policy as follows:
- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or cross cut shredders.

16. Actions upon Termination of Contract

- All St Barnabas MAT equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to St Barnabas MAT at termination of contract.
- All St Barnabas MAT data or intellectual property developed or gained during the period of employment remains the property of St Barnabas MAT and must not be retained beyond termination or reused for any other purpose.

17. Staff Use of Mobile Phones and Smart Devices

- **Professional Conduct:** Staff must ensure that personal mobile phones and smart devices (including smartwatches) are kept on silent and out of sight during directed time, particularly when in the presence of pupils.
- **Personal Use:** Use of personal devices for non-work-related matters is permitted only during designated break times and in staff-only areas (e.g. the staff room).
- **Strict Prohibition of Photography:** Staff are **strictly prohibited** from using personal mobile phones or personal smart devices to take photographs or recordings of pupils, staff, or any school-related activities. Only Trust-sanctioned equipment (such as school iPads or cameras) may be used for capturing images or videos.
- **Security & Authentication:** Where a personal device is required for Multi-Factor Authentication (MFA) to access Trust systems, this must be done discreetly and away from pupils.
- **Communication:** Staff must never use personal mobile numbers or messaging apps (such as WhatsApp) to communicate with pupils or parents. All professional communication must go through official Trust channels.

18. Staff Responsibilities Regarding Generative AI.

- **Human Accountability:** While the Trust **recognises** the value of AI for administrative efficiency, staff remain legally and professionally accountable for any content produced or used. AI-generated materials must be reviewed for accuracy, bias, and appropriateness before being shared or implemented.
- **Data Protection & GDPR:** Staff must **never** input "Personal Data" or "Special Category Data" (as defined by the Data Protection Act 2018) into any AI tool. This includes pupil names, UPNs, addresses, safeguarding concerns, or internal staff records.
- **Academic Integrity:** Staff have a duty to report any suspected misuse of AI by pupils as a breach of academic integrity. When using AI for lesson planning, staff must ensure the content adheres to the Trust's curriculum standards and pedagogical requirements.

- **Safeguarding & Misinformation:** Staff must remain vigilant against AI-generated "deepfakes" and misinformation. Any discovery of AI-generated content that poses a risk to a child or the Trust's reputation must be reported immediately to the **Designated Safeguarding Lead (DSL)**.

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

When using St Barnabas MAT ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's or MAT reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school/MAT, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the school/MAT

I understand that St Barnabas MAT will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use St Barnabas MAT ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Print Name:		**Date:**	
Signed:			