St Ralph Sherwin
Catholic Multi Academy Trust

IT Acceptable Use Policy

Version 2.1
March 2026

One of three Catholic Multi Academy Trusts in the Diocese of Nottingham

Document Provenance

Title of policy:	IT Acceptable Use Policy	
Author and policy owner in the Central Leadership Team:	Trust IT Manager	
Version number:	2.1	
Date approved:	19/05/2026	
Approved by:	Finance and Estates Committee	
Date of next review:	March 2028	
Document review and editorial updates:		
Version control	**Date**	**Key revisions included**
1.0	March 2022	Brand new policy setting out requirements for IT usage
2.0 - draft	January 2025	Updated policy to include AI use, legislative changes, Cyber Essentials compliance, and KCSIE-aligned filtering and monitoring requirements
2.1 - draft	March 2026	Updated policy to comply with JCQ exam regulation requirements.

1. Introduction and Purpose

1.1 This policy establishes specific requirements and best practice guidelines for the appropriate use of information and communication technology (ICT) equipment and facilities throughout The Saint Ralph Sherwin Catholic Multi-Academy Trust (the Trust). This policy applies when working in your usual Academy or office setting and when you are working remotely or travelling.

1.2 ICT is viewed positively by all Trust members as a means of facilitating learning, teaching, research, administration, and approved business activities. Because the Academy's ICT facilities provide a variety of critical services, any attempt to misuse a computer system could result in significant disruption to other Trust users. This could also result in a violation of an individual's data protection rights, causing both the individual and the Trust to suffer harm.

1.3 These facilities are available exclusively for Trust educational purposes. ICT systems are provided for legitimate purposes for which they are intended and for carrying out professional duties. The Trust reserves the right to review and analyse any activity and usage patterns in order to ensure the continued productivity and continuity of the business, without prior notice, to the extent permitted by law.

1.4 The Trust relies on the honesty and integrity of its information technology users, including its own employees and contracted personnel/consultants. The Acceptable Use Policy is not intended to impose restrictions inconsistent with the Trust's established culture of transparency, trust, and integrity. This policy is intended to safeguard all authorised users against illegal or harmful actions taken either intentionally or unintentionally by individuals.

2. Scope

2.1 This policy applies to all Trust employees, contractors, Trust Board Directors, Members, and governors.

2.2 It is the responsibility of all individuals in the Trust to familiarise themselves with this policy and comply with its provisions.

3. Legislation and Regulation

3.1 The Trust is bound in this regard by the provisions of:

- The Data Protection Act 2018 (UK GDPR);
- Human Rights Act 1998;
- Privacy and Electronic Communications (EC Directive) Regulations 2003;
- Regulation of Investigatory Powers Act 2000;

- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;
- Online Safety Bill 2024.

4. General Statement on Acceptable Use

4.1 The user agrees not to upload, download, post, email or otherwise transmit or store anything as follows:

- That is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone's privacy, hateful, or racially, ethically, or otherwise objectionable.
- That the user does not have the right to transmit.
- That infringes any patent, trademark, trade secret, copyright, or other proprietary rights of any party.
- That is unsolicited or unauthorised advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes."
- That contains software viruses, or any other computer code, files, or programs designed to damage computer software, hardware, or telecommunications equipment.
- That is in breach of any other policies that are operating across the Trust.

4.2 Users will also not use the systems to:

- Impersonate any person or entity.
- Interfere with or disrupt the service, servers, or networks connected to the service, or disobey any requirements, procedures, policies, or regulations of networks connected to the service.
- Collect or store personal information about others.
- Undertake any trading, gambling, other action for personal financial gain, or political purposes.
- Store or use any unauthorised software.

4.3 Dormant accounts must not compromise data security. Mechanisms must be in place to ensure secure management.

4.4 IT Support must ensure that all systems made available to staff utilise networks with suitable firewall protection, that virus scanning is installed on all computers, and that operating systems are kept up to date with security patches. Software and operating systems must be supported by the vendor and regularly updated to maintain compliance with Cyber Essentials requirements.

4.5 Employees must not tamper with or circumvent these systems and must notify IT Support immediately if they believe their system is in jeopardy.

4.6 Systems must be set up so that employees only have access to the personal information required to undertake all professional duties in their respective roles.

4.7 Any electronic personal information that could cause harm or distress if lost or stolen must be encrypted (e.g., within a secure management information system or password-protected file). Users are responsible for safeguarding this information when using their own personal devices.

4.8 Any local storage of business data (e.g., computer hard disks) must be encrypted. Where an operating system does not support encryption natively, an appropriate encryption solution must be installed.

4.9. Filtering and Monitoring:

- All internet usage on Trust devices and networks must be subject to robust filtering and monitoring systems to prevent access to harmful content, as required by Keeping Children Safe in Education (KCSIE).

- Filtering systems must block access to illegal, inappropriate, or harmful material, including but not limited to extremist content, pornography, and gambling.

- Monitoring systems should provide alerts for safeguarding risks, including cyberbullying, self-harm, or other welfare concerns, and comply with data protection regulations.

- Physical monitoring by staff of students' use of devices is also essential to ensure compliance with this policy and to uphold safeguarding responsibilities; filtering and monitoring systems implemented are additional tools to aid in monitoring and are never a replacement for physical monitoring by staff.

- IT Support and designated safeguarding leads (DSLs) will review monitoring reports regularly to address potential risks.

5. AI Usage

5.1 **Definition:** Artificial Intelligence (AI) tools include software or platforms that use machine learning or algorithms for generating, analysing, or automating tasks, such as ChatGPT, Google Gemini, or AI-assisted design tools.

5.2 **Prohibited Use by Students:** Students are strictly prohibited from using AI tools, including ChatGPT, Google Gemini and Microsoft Co-Pilot, on school devices. This prohibition aligns with external platform policies, which impose age restrictions on these tools. Refer to individual platform terms for further details.

5.3 **Acceptable Uses for Staff:** Staff may use AI tools for lesson planning, administrative efficiency, and data analysis, provided the output is reviewed for accuracy and does not include confidential information.

5.4 Unacceptable Uses:

- Employing AI to bypass or compromise safeguarding measures, cybersecurity measures such as filtering systems or create harmful material.

- Inputting confidential or personal data into AI systems.

5.5 Guidance and Monitoring:

- Usage may be monitored to ensure compliance with this policy.

6. User and Computer Security

6.1 Each user will be assigned a unique ID (email account) and password for account access. The user is solely responsible for the ID and password, and they **must not be shared with other users or third parties** for any purpose. If it is believed that a user's password has been exposed to anyone, the trust IT Team should be notified immediately

6.2 All Users Passwords should be strong and complex in line with Microsoft 365 password complexity requirements

6.3 All information pertaining to faculty, staff, and students shall be handled in accordance with the Data Protection Act and the data Protection Policies for the Trust and will be shared with only authorised entities and personnel.

6.4 The Trust maintains the right to monitor any network activity (email and files) manually or using automated tools in order to ensure statement compliance and assist in addressing any concerns, in accordance with the law.

6.5 Employees must never disclose account access or passwords. When numerous persons need to access a common account (for example, an enquiries email address), it must be configured so that either one person monitors the account and notifies colleagues, or as an alias where multiple members of staff get correspondence from the shared address.

6.5 Multi-Factor Authentication (MFA) is mandatory for all staff across all systems where this feature is available and feasible, and can be enforced by the Trust IT Team, ensuring enhanced security wherever possible. The Trust will not purchase mobile devices specifically for MFA purposes. Staff are required to install the MFA application on a personal device where a Trust-owned mobile device has not been provided for other purposes. To address privacy concerns, the Trust recommends the use of Microsoft Authenticator and assures that:

- MFA applications do not access or monitor personal data on the device beyond what is required for authentication purposes;
- No personal information from the device will be collected or stored by the Trust;
- The use of MFA applications will comply fully with GDPR and data protection laws.

In cases where staff cannot install an MFA authenticator app, MFA will remain mandatory and non-negotiable. Staff in this scenario must use a fallback option to link their MFA to a mobile phone number, provided this option is approved by the appropriate IT Manager, whether a Network Manager or the Trust IT Manager, and is supported by the platform in question. If the platform requires an authenticator app, staff must comply with this requirement to maintain access.

Staff with questions or concerns about MFA requirements or setup are encouraged to contact their regional IT team or regional Network Manager for guidance and reassurance.

6.6 The Trust IT Team will maintain and regularly review a comprehensive asset register of all Trust-owned devices.

6.7 All devices must be protected with up-to-date anti-malware software and kept fully updated with the latest security patches and software updates.

6.8 Regular backups of information on computer systems must be performed, and copies must be retained in a separate location. Typically, this will be IT Support; nonetheless, employees should ensure that vital files are properly backed up.

6.9 Before disposing of obsolete computers, the Trust assumes that all data has been safely wiped by the user. The Trust IT Team will ensure removal through the use of secure deletion software or physical destruction of the hard disk).

7. Data Protection and Data Security

7.1 All staff are responsible for ensuring that data is handled with care and respect for the rights of our colleagues and the individuals with whom we work at all times, in accordance with the Trust Data Protection Policy.

7.2 When the Trust provides offsite access to systems, the member of staff bears responsibility for ensuring that no one other than the authorised person gets access to the system.

7.3 Moving data across systems is one of the riskiest activities in terms of data security, and extreme caution should always be applied. The ideal way for data transfers is to use the Trust email system or one of the Trust's approved cloud storage solutions. All users must seek direct support and guidance from the IT Support Team if they have any questions relating to sharing and moving information and data.

7.4 External drives, such as USB pen drives (including mobile devices such as smartphones or tablets) should never be utilised for personal or sensitive information. Lesson resources and other related material must be stored on OneDrive, Teams or SharePoint and can be synced with a Trust device for offline access. Data from devices should be securely transferred via OneDrive or SharePoint Cloud platforms wherever possible to avoid a direct USB connection to PCs. In exceptional circumstances a USB may be used under the direct supervision of the Trust IT Support Staff.

7.5 If it is absolutely necessary to use a USB for teaching and learning then it should only be for as short a period as possible and the local drive must be encrypted.

7.6 Data will be processed to be in line with our requirements and protections set out in the UK General Data Protection Regulation, Data Protection Act as amended by the Data (Use and Access) Act 2025.

8. Equipment Handling and Care

8.1 Equipment is given for the purpose of carrying out your professional activities and must be handled with care at all times.

8.2 Staff must return equipment at the end of their employment with the Trust. This will be logged, dated and signed so that as part of the return of equipment the IT Support Team can disable logins to all Trust systems.

9. Internet Services

9.1 The Trust expects users to use the internet responsibly and to report any objectionable material to the appropriate authority; this may be to the academy senior leadership team and / or relevant regional IT support team.

9.2 Accessing offensive material via the internet, whether on Trust-owned equipment or during work hours, is a significant disciplinary offence and will be investigated in accordance with the Disciplinary Policy.

9.3 Because employees may use the internet via a variety of public and private networks, it is critical that staff exercise sound professional judgement when using the internet.

10. File Storage and File Management

10.1 Files will be stored either on a Trust provided system with appropriate file-security, on a Trust approved network file store or, by prior agreement on a third-party system which meets the minimum-security requirements agreed by the Trust and must have a DPIA in place.

10.2 This includes the use of unencrypted external USB storage of any kind which may not be used on any Trust IT system without previous written authorisation from a Trust Network Manager.

10.3 Any sensitive information to be emailed or otherwise transmitted outside the Trust must be encrypted to a standard agreed in advance with IT Support.

10.4 Files must never be stored on a public-access file store system not approved by the Trust.

10.5 There are various cloud services in use by the Trust within the CMAT system. Staff are required to only use those services that are supported by the Trust, secured by their business login (either @srscmat.co.uk or @*.srscmat.co.uk where * represents a relevant three-character school code) and in line with the trust Data Protection Policy.

10.6 Trust email accounts must not be used to sign up or login to services that are solely for personal use, such as personal shopping accounts or personal mailing lists.

10.7 It is not acceptable under any circumstances to use a personal cloud storage account (e.g., a personal Dropbox, Apple iCloud, OneDrive or Google Drive) to handle Trust data.

11. Electronic Mail Services

11.1 Information held in a Trust administered email system is the property of the Trust.

11.2 All Trust staff, governors and Trust Board Directors that require email access as part of their professional duties will be provided with a business email address using the Trust approved service. The email address will be suffixed with 'srscmat.co.uk'.

11.3 Personal email addresses **must not** be used to transact Trust business except in an emergency situation where a rapid response is required, and the proper service is unavailable. When a personal address is used, a copy of the message must be sent to the relevant business address so that an audit trail is maintained.

11.4 Emails of a confidential or sensitive nature must be clearly marked in the subject line so that the recipient is made aware. Sensitive information should be sent as a secure link rather than in the body of an email.

12. Media Rights and Licenced Content

12.1 Often files that can be purchased or rented privately (music, films, etc.) are licenced in such a way that their storage or transmission over a corporate network is prohibited.

12.2 Users must not use media purchased on our systems unless they are certain they are not in violation of the licence agreement they entered into with the owner when they purchased that content.

13. Using Social Media

13.1 When using social media, whether professionally or privately, staff should ensure that the content associated with them is consistent with their work at the Trust - exercise professional discretion in all personal communications on social media, include a disclaimer when using social media for personal purposes, and must avoid using the SRSCMAT email address, logos, or other identifying information, making it clear that what you say represents your personal views only.

13.2 Any derogatory comments on social media platforms that expressly or impliedly criticise the Trust, it's employees, pupils or a relevant third party may be cause for disciplinary action.

14. Bringing Your Own Device to Work ("BYOD")

14.1 All personal devices used for professional purposes are subject to the following conditions:

- If a computer, smartphone, or tablet is connected to the Trust's information technology systems or contains Trust-owned data, it is subject to the same Acceptable Use policies as the Trust's own equipment, regardless of who owns it;

- The Trust is not responsible for the device's storage, maintenance, or security;

- No attempt may be made to circumvent the Trust's security and filtering procedures. Before connecting to Trust systems, including Wi-Fi, any personal mobile device must be secured with a PIN Code and all available security mechanisms enabled. Wherever practicable, any device connected to the Trust systems is expected to be under the oversight or awareness of the IT Team. Where this is not practicable, any device connected to Trust systems must have all current security patches updated and a recognised antivirus system installed prior to connecting to the Trust system; this is the owner's duty. Any device that does not match this criterion will be automatically withdrawn from the Trust systems. Security systems and passwords are subject to change at any time, necessitating the reconnecting of personal devices;

- It is the owner's responsibility to ensure that the equipment is safe to use;

- The Trust maintains the right to revoke access to its systems at any time and without prior notice;

- Any personal device that is used to store Trust data (including emails) must be password- or passcode-protected (failure to do so would be misconduct);

- At no point in time may confidential or personal data (including that covered by the Data Protection Policy) be stored on a personal device.
- When an employee leaves the Trust, data relating to their employment with us will be automatically removed from the device.

- Personal devices' cameras must never be used to photograph or record students.

- Devices not managed by the Trust (i.e., those not wiped and configured solely for work purposes) must connect to an isolated guest network that prevents communication with devices on the secure main network.

- The Pre-Shared Key (PSK) for the secure internal network is exclusively managed by the IT department and is not shared with non-IT staff or students. All authorised Trust-managed devices will be configured to connect automatically to the secure network. Schools and users are only permitted to connect unmanaged devices to the isolated guest network. The guest network is for personal devices belonging to staff and guest devices only and must never be used by students.

15. Mobile Devices and Smartphones

15.1 Mobile devices can represent a security risk, particularly "passive loss" of data, which occurs when a staff member has a smart phone or tablet set up to receive corporate email or store files in some way.

15.2 To reduce risk, any mobile device with a Trust email address must have a PIN lock activated; if this is not available, a Trust email address should not be used with that device. Staff must be aware that intentionally enabling access to their Trust email on an insecure device without taking precautions to protect it is a violation of the Trust IT Acceptable Use Policy.

15.3 If a device containing Trust data (including email) is lost, user must notify Trust IT Support immediately so that we can remotely erase any sensitive data from the device. Any loss of data must also be reported to the GDPR lead in each academy, the Trust IT Manager and to the DPO for the Trust.

15.4 The Trusts' IT Support Team will register mobile devices on the Trust systems so that if a device is lost or stolen, it can be remotely deleted.

16. Responsibilities

16.1 The Trust recognises that staff awareness is a key element of maintaining strong cyber security. All Staff are required to complete regular cyber security awareness training to ensure they understand current threats and safe working practices when using Trust IT Systems

16.2 All Trust employees, contractors, Trust Board Directors, Members and governors, have a responsibility to follow this policy and take time to read and understand this policy.

16.3 The Headteacher is responsible for making certain that all staff and governors have read and understood this policy. The Trust IT Manager and Trust Support Teams will support with training and updates to help everyone understand and adhere to the policy.

16.4 The Trust IT Manager is responsible for ensuring that the all staff working in the Trust central teams and their line mangers have read and understood the policy and know how to adhere to it.

17. Monitoring, Compliance and Review

17.1 The responsibility for monitoring and reviewing the impact of this policy and making recommendations sits with the IT Manager for the Trust.

17.2 The Finance and Estates Committee will review and sign off this policy every two years unless within the two-year window there are legislation changes and requirements that mean that the Trust has to update the policy.

Summary of Changes (to be removed in final release version)

Document Provenance

Version Details:

- **Version 1**: Dated March 2022, described as the "brand new policy."
- **Version 2**: Updated to January 2025, adding key revisions such as AI use, legislative changes, Cyber Essentials compliance, and KCSIE-aligned filtering/monitoring requirements.

Review Dates:

- **Version 1**: Next review scheduled for March 2024.
- **Version 2**: Updated to January 2027.

Section 3: Legislation and Regulation

Addition in Version 2:

- Inclusion of the **Online Safety Bill (2024)**.

Section 4: General Statement on Acceptable Use

Filtering and Monitoring:

- **Version 2 Additions**:
  1. Detailed compliance with KCSIE.
  2. Clarified that filtering and monitoring systems are supplemental tools and not replacements for physical monitoring by staff.

Section 5: AI Usage (New in Version 2)

1. **Definition**:
   - Detailed AI tools such as ChatGPT, Google Gemini, and Microsoft Co-Pilot.
2. **Prohibited Use**:
   - Students are explicitly prohibited from using AI tools on Trust devices, aligning with platform-imposed age restrictions.
3. **Acceptable Uses for Staff**:
   - Defined permissible uses, such as lesson planning and administrative efficiency, with accuracy reviews required.
4. **Unacceptable Uses**:
   - Prohibited misuse of AI tools, including bypassing safeguards and inputting confidential data.

5. **Guidance and Monitoring**:
    - Usage subject to monitoring to ensure compliance

Section 6: User and Computer Security

1. **Multi-Factor Authentication (MFA)**:
    - **Version 2 Enhancements**:
        - Mandatory MFA for all staff wherever it available and feasible.
        - Trust will not purchase mobile devices for MFA; staff must use personal devices unless a valid exemption is approved.
        - Fall-back option introduced for linking MFA to a mobile number where approved and supported by the platform.

Section 7: Data Protection and Data Security

1. **USB and External Drives**:
    - **Version 2 Expansion**:
        - Usage restricted to exceptional circumstances, supervised by IT Support.
        - Stronger emphasis on encryption for lesson resources when USB use is unavoidable.
        - Expanded to avoiding connecting mobile devices to PCs via direct USB connection and emphasising need for secure transfer of data via Cloud platforms such as OneDrive or SharePoint wherever possible.

Section 13: Bringing Your Own Device (BYOD)

1. **Enhanced BYOD Requirements**:
    - **Version 2 Additions**:
        - Explicitly highlights the requirement for “personal” devices and other non-Trust managed devices to be connected to a secure Guest network which prevents connectivity with internal services and other Trust-owned devices.
        - Added a requirement that the Pre-Shared Key (PSK) for the secure internal network is exclusively managed by the IT department and not shared with non-IT staff or students. This ensures only Trust-managed devices can connect to the secure network, while unmanaged devices are restricted to the isolated guest network.
        - Clarified that the isolated guest network is for staff devices only and must not be used by students.