St Ralph Sherwin
Catholic Multi Academy Trust

IT Acceptable Use Policy

Version 1
March 2022

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

St Ralph Sherwin
Catholic Multi Academy Trust

Document Provenance

Title of policy:	**IT Acceptable Use Policy**	
Author and policy owner in the Executive Team:	IT Manager	
Version number:	1	
Date approved:	8 March 2022	
Approved by:	Finance and Estates Committee	
Date of next review:	Every two years – March 2024	
Document review and editorial updates:		
Version control	**Date**	**Key revisions included**
Version 1	March 2022	This is a brand new policy setting out requirements across our Trust and ensuring we have full compliance with securing effective and compliant IT usage.

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. 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);
- European Human Rights Legislation;
- The Privacy and Electronic Communications (EC Directive) Regulations 2003; ✦ The Regulation of Investigatory Powers Act 2000.
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000[9].

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 or 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. When an account becomes dormant, either because someone has left the Trust or is absent for an extended period of time, the mechanisms put in place must not jeopardise data security.

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.

4.5. Employees must not tamper with or circumvent those systems and must notify IT Support 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 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 when using their own personal devices.

4.8. Any local storage of computer systems used to retain any business data (for example, a computer hard disc) must be encrypted. When using an operating system that does not support this as a standard feature, a strong encryption replacement must be installed.

5. User and Computer Security

5.1. 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.

5.2. 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

5.3. 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

5.4. 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.

5.5. Staff user accounts may be set up or moved to Two Factor Authentication (2FA) at any time if the Trust IT Support Team so directs. Trust accounts now have an extra degree of security. The trust is working towards all staff accounts to be configured with MFA, whenever practicable, for access to Trust-based systems.

5.6. 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.

5.7. 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).

6. Data Protection and Data Security

6.1. 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.

6.2. 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.

6.3. 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.

6.4. External drives (such as USB pen drives) 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. In exceptional circumstances a USB may be used under the direct supervision of the Trust IT Support Staff, who will ensure encryption is enabled.

6.5. 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. Equipment Handling and Care

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

7.2. 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.

8. Internet Services

8.1. The Trust expects users to use the internet responsibly and to report any objectionable material to the appropriate authority; if based in an Academy report this to the academy senior leadership team and IT support in the academy, and if in the centrally based Trust teams report this to the Trust IT Manager.

8.2. 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.

8.3. 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.

9. File Storage and File Management

9.1. 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.

9.2. 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.

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

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

9.5. 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 @<school initials>.srscmat.co.uk) and in line with the trust Data Protection Policy.

9.6. 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.

9.7. 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.

10. Electronic Mail Services

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

10.2. 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'.

10.3. 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.

10.4. 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.

11. Media Rights and Licenced Content

11.1. 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.

11.2. 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.

12. Using Social Media

12.1. 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.

12.2. 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.

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

13.1. 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.

14. Mobile Devices and Smartphones

14.1. 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.

14.2. 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.

14.3. 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.

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

15. Responsibilities

15.1. 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.

15.2. 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

15.3. 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.

16. Monitoring, Compliance and Review

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

16.2. 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.