St Gabriel
the Archangel
Catholic Multi-Academy Trust

INFORMATION AND CYBER SECURITY POLICY

POLICY TO BE REVIEWED EVERY YEAR OR EARLIER DUE TO ANY LEGISLATIVE CHANGES

FOR ALL ACADEMIES PART OF ST GABRIEL THE ARCHANGEL CATHOLIC MULTI-ACADEMY TRUST

Approved by Audit and Risk Committee 23rd April 2026

Next Review: April 2027

1. Purpose

St Gabriel the Archangel Catholic Multi-Academy Trust ("the Trust", "SGtACMAT") Information Security Policy outlines the Trust's guidelines and provisions for preserving the security of the Trust's data and technology infrastructure, including but not limited to, a cyber attack.

All information held by the Trust, in all formats, represents an extremely valuable asset and therefore, must be used, stored and if required, transmitted, in a secure manner. In accordance with DfE Cyber Security Standards, this infrastructure encompasses all cloud-hosted environments; including but not limited to, Microsoft 365, Google Workspace, and Azure, local area networks and third-party SaaS (Software-as-a-service) platforms used for Finance, HR and MIS.

Human error, cyber attacks and system malfunctions could not only cause great financial impact and reputational damage, but may also affect teaching and learning and compromise our UK GDPR compliance. For this reason, we have implemented a number of security measures and have prepared instructions that may help mitigate security risks.

2. Scope

This policy applies to all directors, governors, employees, contractors, volunteers and anyone who has permanent, or temporary, access to our systems and hardware. It applies to all locations from which systems are accessed, including remote and home use. The scope extends to all Trust provided software, hardware and digital assets regardless of the service provider.

This policy must be read in conjunction with the following policies:

ICT Acceptable Use Policy
Data Protection Policy

3. Policy Objectives

1. To ensure all employees are aware of and comply with relevant legislation and associated policies.
2. To maintain a high level of cyber security awareness across the Trust.
3. To ensure the Trust meets the DfE Digital Standards for Cyber Security.

4. Privacy by Design

Privacy by design is an approach to projects that ensures privacy and data protection compliance are considered and implemented at the earliest stage of development. The UK General Data Protection Regulation (UK GDPR) introduces a legal requirement for Data Protection Impact Assessments (DPIA) to be completed to ensure privacy by design. St Gabriel the Archangel Catholic Multi-Academy Trust will therefore ensure

that privacy and data protection is a key consideration throughout the lifecycle of a project. Such projects would include:

- A new IT system for storing and accessing personal information
- A new data sharing process
- Introduction of a new CCTV system or the addition of new technology to an existing system (for example adding Automatic Number Plate Recognition (ANPR) capabilities to existing CCTV).
- The introduction of Artificial Intelligence (AI) tools.

5. Access Control & Identity Management

Those users within the scope of this policy must only access systems for which they are explicitly authorised. Unauthorised access attempts are a criminal offence under the Computer Misuse Act (1990).

Leavers: Upon termination of employment, access must be removed immediately from all systems, including the network, Microsoft 365, Google Workspace, Azure, Arbor, and Finance systems.

Privileged Access: Administrative accounts must be strictly controlled and kept separate from day-to-day user accounts. This ensures that a compromise of a standard user account does not grant an attacker full system control.

Multi-Factor Authentication (MFA): MFA is mandatory for all employees across all cloud services (Microsoft 365, Google Workspace, Finance systems, etc.) without exception.

6. Security of ICT Equipment

6.1. Trust Issued ICT Equipment

A key principle of the DfE Cyber Security Standards and UK GDPR is for organisations to implement appropriate technical and organisational measures in order to ensure data security. The Trust is committed to securing data at all times. All Trust employees and Directors/Governors with company equipment are responsible for ensuring that the following guidelines are followed at all times:

- All portable computers have appropriate access protection ensuring passwords meet the minimum password complexity policy, as set out in section 10 of this policy.
- Portable computers must not be left unattended in public places.
- Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and other electronic equipment when leaving an office unattended and lock equipment away when you are leaving the office.
- When leaving a computer/laptop unattended ensure that the screen is locked, turned off or has been logged out.

- Portable computers must never be left unattended in cars.
- Do not leave any devices (personal or Trust owned) exposed or unattended outside the Trust premises.
- Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times. The equipment must only be used by the individual to which it is issued, be maintained and batteries recharged as required.
- Staff working from home must ensure appropriate security is in place to protect Trust equipment or information. This will include physical security measures to prevent unauthorised entry to the home, and ensuring Trust equipment and information is kept out of sight.
- Trust issued equipment must not be used by non-Trust employees.

The IT Support team are responsible for ensuring the following:

- That all users have the means to update their password, enforcing password policies to ensure they meet the minimum password requirements. The password complexity policy is detailed in section 10 of this policy.
- All high-risk or critical security updates for operating systems (Windows, ChromeOS, iOS) and applications must be applied within 14 days of release to comply with DfE standards.
- All data carried on portable computers is encrypted.
- All portable computers have an adequate level of endpoint protection, including, but not limited to:
    - Endpoint protection/antivirus; real-time scanning and remediation
    - Application control
    - Peripheral control
    - Data loss prevention

6.2. The use of personal ICT Equipment

The use of personal ICT equipment is strictly prohibited for accessing Trust systems, with the exception of Google Workspace Email access as outlined in section 7 of this policy.

7. Cloud and Email Access

7. Trust issued accounts

Employees, directors and governors of St Gabriel the Archangel Catholic Multi-Academy Trust can use the Gmail App (available for iOS and Android) to access Trust emails for Google Workspace. The Trust has implemented appropriate technical measures in order to protect data using the aforementioned apps. Access on mobile devices is only permitted in accordance with the following terms:

- The Gmail app is the only permitted route of access to emails for the Google Workspace service.

- A suitable passcode, biometric, FaceID or similar form of security measure is in place on the mobile device accessing a Google Workspace account.
- 2-Factor Authentication (MFA/2FA) is required for access to all cloud services (Microsoft 365, Google Workspace, Azure, Finance systems) for all employees, without exception.

7.2 Suspicious Emails and content

Trust owned laptops are secured with the latest endpoint protection suite of products, that actively monitor for suspicious files and activity. Emails can host scams, which are undetectable by endpoint protection suites, and malicious software. To avoid virus infection (or similar) or data theft employees should:

- Avoid opening attachments and clicking on the links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of 'clickbait' titles (e.g. offering prizes or advice.)
- Be suspicious of incorrectly spelt attachments.
- Look for inconsistencies (e.g. spelling/grammar mistakes, capital letters and/or excessive use of punctuation.)
- Check the email address of the sender is spelt correctly.
- Be suspicious of urgent calls to action ("Please make this payment within the hour" or "I can't talk now, can you send this money to X")
- Be suspicious of threats ("act within 1 hour to claim a reward")

Regard any emails that meet the following criteria with particular suspicion:

- If they come from someone you don't know, who has no legitimate reason to send them to you.
- If an attachment arrives with an empty message.
- If there is some text in the message, but it doesn't mention the attachment.
- If there is a message, but it doesn't seem to make sense.
- If there is a message, but it seems uncharacteristic of the sender.
- If the message doesn't include any personal references at all, (for instance a short message that just says something like "You must take a look at this", or "I'm sending you this because I need your advice").
- If it has a filename with a 'double extension', like FILENAME.JPG.vbs or FILENAME.TXT.scr, that may be extremely suspicious.

If you are unsure if an email is legitimate, you must refer it to the IT Support team immediately by emailing the helpdesk.

Newly appointed staff, directors and governors will be provided with access to cyber security awareness training, which will include sections on email security. This training is mandatory and must be completed annually. Access to Trust systems will only be provided once this training has been completed.

8. The use of portable storage devices

St Gabriel the Archangel Catholic Multi-Academy Trust prohibits the use of portable storage devices including, but not limited to, USB memory sticks/flash drives and USB hard drives, for the transfer of data from Trust systems to a portable storage device. USB storage devices are blocked and cannot be used on Trust owned devices, with exception of examination requirements; this process will be reviewed by the IT Director and will be agreed for a specified amount of time. This is a technical measure implemented to ensure the control of data, inline with the Trust's UK General Data Protection Regulation policy and to mitigate cybersecurity threats. The use of the Trust provided Google Drive service is encouraged.

9. The use of cloud storage services

The use of third party cloud storage solutions (for example Skydrive, iCloud, Dropbox, Box, Sync, Mega etc.) for the transfer or storage of Trust information is strictly forbidden. Access only to the following authorised cloud services for the storage of Trust information, in line with the Trust's Data Protection policy, are permitted:

- Google Drive
- Microsoft OneDrive for Business

10. Managing passwords

Weak passwords, writing passwords down or sharing passwords with others is dangerous as this can compromise the security of the entire IT infrastructure. Not only should passwords be secure to prevent an individual from guessing, but they should also remain secret. For this reason, we enforce the following password complexity requirements:

- Minimum of 8 characters
- The password contains characters from three of the following categories:
    - At least 1 number
    - At least 1 non-alphanumeric character (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) Currency symbols such as the Euro or British Pound aren't counted as special characters for this policy setting.
    - At least 1 capital letter
    - At least 1 number
- The password must not contain your name or username.

Accounts will be locked after 5 failed login attempts (the member of staff must then contact IT Support to unlock the account).

In line with NCSC guidance, we do not require regular changing of passwords. The use of "three random words" is encouraged to create long, secure, and memorable passwords.

11. Transferring data securely

- The use of removable storage devices is prohibited.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft or loss.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by email or any other form of electronic communication, staff will always check that the recipient is correct before sending and consideration is made as to whether the use of Gmails 'confidential' mode is appropriate and/or the attachments are password protected.

Before sharing data, all staff members must ensure:

- They are allowed to share it. Referring to the UK General Data Protection Regulation policy and the Trust's Data Protection Officer.
- That adequate security measures are in place to protect the data.
- The recipient is UK GDPR compliant.

Under no circumstances are visitors allowed access to confidential or personal information.

12. Additional Security Measures

The security and ongoing protection of the Trust infrastructure is of paramount importance to the Trust. To reduce the likelihood of security breaches employees must:

- Lock their device when leaving their desk.
- Report stolen or damaged equipment as soon as possible to the Director of IT.
- Report a perceived threat or possible security weakness in the Trust's systems to the Director of IT without delay. Responsible reporting ensures that vulnerabilities can be addressed without compromising the security of the Trust.
- Refrain from downloading suspicious, unauthorised or illegal software on Trust equipment.
- Avoid accessing suspicious websites.

The IT Support Team are responsible for:

- Managing firewall restrictions, filtering software, endpoint protection suite, monitoring software and access authentication systems.
- Investigating and recording security breaches.

- Following this policies requirements, as expected of all staff.
- Ensure the Trust has physical and technological safeguards in place to protect information.

13. 2 Factor Authentication (2FA)

The use of 2 factor authentication adds an additional layer of security by adding a second form of authentication required in order to access a service, rather than simply a username and password. An example of 2FA is when making a payment via an online bank, you will be sent a one time password/pin (OTP) to your mobile phone to enter on the website to authorise the payment. 2FA is used to enhance the security measures that we have in place for password complexity requirements, etc. by prompting the user to enter a pin sent to their mobile phone at the point of login, the use of 2FA makes it more difficult for an attacker to access a user's account.

MFA is mandatory for all employees across all cloud services (Microsoft 365, Google Workspace, Finance systems, etc.) without exception.

2FA codes are not required for every login but issued after a period of time, an unusual pattern of login (e.g. multiple login attempts), a new location or a new/unrecognised device.

14. Data Resilience and Backups

The IT support team must ensure the system is backed up regularly. Backup restoration processes must be tested and recorded at least termly to ensure the Trust can recover if the need arises.

The Trust and associated schools must follow the NCSC "3-2-1" backup rule: at least 3 copies of data, on 2 different media types, with at least 1 copy kept in a logically or physically disconnected/immutable cloud environment.

15. Monitoring of account activity

Activity of staff and student accounts is recorded for the purpose of safeguarding and security and includes the following information:

- Log in/Logout of account
- Access and activity within cloud services (e.g. documents that have been created, edited and shared)
- All inbound and outbound emails (including attachments)
- All Hangouts/Chat/Teams communication
- All Google Meet/Teams events

Internet activity is recorded and retained for a period of time to allow suspicious activity to be investigated. Suspicious activity includes search terms containing, but not limited to, extremist ideology or pornographic vocabulary. Activity can be reported on by the IT support team at the request of the Trust's safeguarding team or senior management team.

16. Unmanaged device network access

Access to an academy network is only provided for organisation owned and managed devices. Access will not be provided for personal devices, including mobile phones or laptops.

17. Updates

Updates for products and services are managed centrally. Staff and student devices are configured to install Windows, Chrome and endpoint security updates automatically outside of the school day. Staff and students must allow updates to be installed and they may be prompted to restart their device to finish the installation of updates.

Devices that no longer receive security updates from the manufacturer will be retired (see section 20 for more information) and disposed of in accordance with the Trust's asset management policy and in line with WEEE regulations.

19. Firewall and Internet Filtering

Automated procedures are in place to check the network for 'unauthorised' files. The IT support team must ensure that an adequate firewall and filtering service are employed to restrict external access and activity to the Trust's IT network and to protect the Trust from cyber vulnerabilities.

20. Cyber Security Training

All employees must undertake annual cyber security awareness training. Access to Trust systems will only be provided once this training has been completed.

21. End-of-life (EOL) devices

SGtACMAT is committed to maintaining a secure IT environment. A critical aspect of this commitment is ensuring all devices on our network are up-to-date with the latest security patches and fixes.

End-of-Life (EOL) refers to devices that manufacturers no longer actively supports; meaning the manufacturer will cease providing critical security updates and patches, leaving the devices vulnerable to known and unknown security exploits and includes, but is not limited to:

- Laptops/desktops
- iPads/tablets
- Chromebooks
- Network switches/routers/firewalls
- Access points
- Servers

To mitigate these risks, SGtACMAT will:

- Maintain an asset register of all devices used on our network
- Monitor the EOL status of devices
- Retire the device from use and where applicable replacing it with a supported model.

By proactively managing EOL devices, we can significantly reduce the attack surface of our network and subsequently protect sensitive information.

22. Artificial Intelligence

- The Trust recognises the importance of equipping learners and staff with the knowledge, skills and strategies to engage responsibly with AI tools.
- Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. **Personally identifiable or sensitive information should never be input into AI tools.**
- Only those AI technologies approved by the school may be used.
- **Staff must not input sensitive information, such as student information or internal documents, into AI tools. Staff must always recognise and safeguard sensitive data.**
- Staff must ensure that when AI is used, it does not infringe copyright or intellectual property conventions – care must be taken to protect intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. **Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately** to the Trust DPO (Mrs B Raj). Quick reporting helps mitigate risks and facilitates a prompt response.

Version	Approval Date	Action/Notes	Signature of the Chair of Committee/Board
1	23/04/2026	Approved by A&R Committee	*P Rushworth*