SANCTA FAMILIA
CATHOLIC ACADEMY TRUST

Cyber Security Policy

Internal Use

Policy Owner:	CEO
Review Cycle:	Annually
Date of last review:	September 2025
Date of next review:	September 2026

Contents

Introduction and aims of this policy 3
Scope 3
Roles and Responsibilities 3
Risk Management 3
Physical Security 3
Asset Management 4
User Accounts 4
Devices 4
Data Security 5
Sharing Files 5
Training 5
Cyber Security Compliance for External Users 6
System Security 6
Major Incidents Response Plan 6
Cyber Insurance 6

Introduction and aims of this policy

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection. This Cybersecurity Policy outlines Sancta Familia Catholic Academy Trust guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Scope

This policy applies to all Sancta Familia Catholic Academy Trust staff, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Roles and Responsibilities

- The Chief Executive Officer (CEO): Accountable for overall cyber security governance.
- Each school retains responsibility for its Cyber Security, however it is expected that each school will have a policy that reflects this policy requirements as a minimum.
- Data Protection Officer (DPO): Ensures compliance with data protection legislation.
- All Staff: Responsible for following cyber security protocols and reporting incidents.
- Staff should report all incidents as soon as possible to their Headteacher, or in case they are not available, the Deputy Headteacher or School Business Manager.
- The Headteacher, or delegate, should then inform the incident to the CEO or they are not available, the CFO – without delay.

Risk Management

Sancta Familia Catholic Academy Trust will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to Trustees annually.

Physical Security

Sancta Familia Academy Trust will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms. Physical security systems will be reviewed periodically to ensure best practice.

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, Sancta Familia Catholic Academy Trust will maintain asset registers for: files/systems that hold confidential data; and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform their IT Service Desk as soon as possible. Personal accounts should not be used for work purposes. Sancta Familia Catholic Academy Trust will work with colleagues across the Trust to ensure multifactor authentication is in place across all devices as soon as possible.

Devices

To ensure the security of all Sancta Familia Catholic Academy Trust issued devices and data, users are required to:

- Lock devices that are left unattended
- Update devices when prompted but only when from a trusted source e.g. IT department. If unsure, please do not update and contact your IT department as soon as possible to confirm and then update.
- Report lost or stolen IT equipment as soon as possible to your Headteacher, Deputy Headteacher, or School Business Manager as
- Change all account passwords at once when a device is lost or stolen (and report immediately to the IT Service Desk or IT provider)
- Report a suspected threat or security weakness in Sancta Familia Catholic Academy Trust's systems to your Headteacher, Deputy Headteacher, or School Business Manager as soon as possible.

Devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts
- Access controls

Data Security

Sancta Familia Catholic Academy Trust will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Sancta Familia Catholic Academy Trust defines confidential data as:

- Personally identifiable information as defined by the ICO
- Special Category personal data as defined by the ICO
- Unpublished financial information

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology:

- 3 versions of data
- 2 different types of media
- 1 copy offsite/ offline

Sharing Files

Sancta Familia Catholic Academy Trust recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a date breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Wherever possible, keeping Sancta Familia Academy Trust files on school systems
- School files should not typically be sent to personal devices unless there is an express need to do so
- Verifying the recipient of data prior to sending
- Using file encryption where possible, sending passwords/keys via alternative communication channels
- Alerting the Headteacher / Deputy Headteacher / Business Manager as soon as possible regarding any breaches, malicious activity or suspected scams

Training

Sancta Familia Catholic Academy Trust recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

Cyber Security Compliance for External Users

Sancta Familia Catholic Academy Trust recognises the importance of ensuring that all individuals granted access to Trust systems – including visitors and external hirers – comply with its Cyber Security Policy. As part of the lettings and visitor management process, external users are required to acknowledge and adhere to relevant cyber security protocols prior to accessing any Trust hardware or systems. This includes restrictions on network access, appropriate use of devices, and safeguarding of data. Guest access is segregated from core school systems and monitored to prevent unauthorised activity. Where regular access is granted, appropriate training or guidance will be provided to ensure understanding of responsibilities. These measures are reviewed periodically to maintain the integrity and security of Trust IT infrastructure.

System Security

Security principles will be built into the design of IT services covering but not limited to:

- Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors' & staff personal devices from school systems
- Review the security risk of new systems or projects

These principles to be applied across all academies as well as Trust Central IT services.

Major Incidents Response Plan

Sancta Familia Academy Trust will develop, maintain, and regularly test a Cybersecurity Major Incident Response Plan. This will include identifying or carrying out:

Key decision-makers

- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g. IT support company)

Cyber Insurance

Sancta Familia Academy Trust will maintain appropriate cyber insurance coverage to mitigate financial risks associated with data breaches, ransomware, and other cyber incidents.

SANCTA FAMILIA
CATHOLIC ACADEMY TRUST

Website: www.sanctafamilia.co.uk
Email: info@sanctafamilia.co.uk
Registered in England, Company Number: 15116317

UID: 17728
UKPRN: 10094584