Cyber Security Policy

Saint Marys Catholic Primary School

Approved by:

Last reviewed on: December 2025

Next review due by: December 2027

Introduction

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 Saint Mary's Catholic Primary School guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack. Computeam/One Education are our IT support services who we work closely with to maintain and protect our infrastructure.

Scope of Policy

This policy applies to all Saint Mary's Catholic Primary School's 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.

Risk Management

CyberSecurity risks are recorded by the OLHOC Academy Trust and are discussed in the Governor meetings and with our IT and security providers.

Physical Security

Saint Mary's Catholic Primary School will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to lockable cabinets, and secure server/communications rooms.

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, Saintt Mary's Catholic Primary School will maintain asset registers for, files/systems that hold confidential data, and all physical devices (services, 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 Computeam, One Education and OLHOC as soon as possible. Personal accounts should not be used for work

purposes. Saint Mary's Catholic Primary School will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all Saint Mary's Catholic Primary School issued devices and data, users are required to:

- Lock devices that are left unattended
- Update devices when prompted
- Report lost or stolen equipment as soon as possible to the School Business Manager who will inform OLHOC and Computeam/One Education.
- Change all account passwords at once when a device is lost or stolen. Report immediately to the Office Manager/SLT who will inform OLHOC and Computeam/One Education.
- Report a suspected threat or security weakness in Saint Mary's Catholic Primary School's systems to Office Manager/SLT who will inform OLHOC and Computeam/One Education.

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

- Password protection
- Full disk encryption (if required and is recommended if data is stored on the device).
- Client firewalls
- Anti-virus / malware software
- Automatic security updates
- Removal of unrequired and unsupported software that we notify Computeam/One Education of.
- Minimal administrative accounts

Data Security

Saint Mary's Catholic Primary School will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Saint Mary's Catholic Primary School 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

Saint Mary's Catholic Primary School recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a data 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 files on school systems.
- Not sending school files to personal accounts.
- Verifying the recipient of data prior to sending.
- Using file encryption where possible, sending passwords/keys via alternative communication
- Channels.
- Alerting [IT Support/DPO] to any breaches, malicious activity or suspected scams.

Training

Saint Mary's Catholic Primary School recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training using SMARTLOG training, 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.

System Security

Computeam/One Education will build security principles into the design of IT services for Saint Mary's Catholic Primary School;

- Security patching – operating systems, network attached storage 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

Major Incident Response Plan

Saint Mary's Catholic Primary School and Computeam/One Education 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 arestored 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)

Maintaining Security

Saint Mary's Catholic Primary School understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems.

Saint Mary's Catholic Primary School will budget appropriately to keep cyber related risk to a minimum.

Head Teacher:	Amy Butterfield
Chair of Governors:	Val Bridge
Technical Support:	One Education/Computeam

Date this policy was reviewed and by whom:

Date of next review and by whom