St. Mark's Catholic Primary School

Cyber Security Policy

Written by: Knowsley MBC	**Approval level:** Headteacher / Chair of Governors
Approved by: *Catherine Ming*	**Review date**: September 2026

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 loss of sensitive personal information, loss of student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cyber Security Policy outlines St. Mark's Catholic Primary School's objectives, guidelines, and security provisions, designed to protect our systems, services, and data in the event of a cyberattack, ensure compliance with the DfE's 'Meeting digital and technology standards in schools and colleges, 'and promote continuity of learning.

Scope of Policy
This policy applies to all school staff, contractors, volunteers, and anyone else granted permanent or temporary access to our systems, hardware, and digital learning resources. It also covers the physical, digital, and technical elements that are used to deliver IT services for the school, including any third-party services.

Risk Management
Cybersecurity risks will be included in St. Mark's Catholic Primary School's organisational risk register and reported on to Governors twice a year. The school will regularly assess and update the risk register, prioritising mitigation strategies and keeping key stakeholders informed.

Physical Security
Appropriate physical security and environmental controls will protect access to IT Systems, including air conditioning, lockable cabinets, secure server/communications rooms, and restricted access to sensitive areas.

Asset Management
St. Mark's Catholic Primary School will maintain comprehensive asset registers for:

- All files/systems that hold confidential data
- All physical devices (servers, switches, desktops, laptops, etc.) comprising its IT infrastructure
- Security controls will be applied to protect data and systems effectively, ensuring an accurate, up-to-date record of all assets.

User Accounts

- **User Responsibility:** Users are responsible for the security of their accounts. If they suspect their credentials may be compromised (e.g., after a phishing attempt), they must change their password and inform IT Support immediately. Personal accounts must not be used for work purposes.
- **Password Standards:** Users must use complex passwords that meet or exceed minimum school-defined requirements and change passwords in line with current NCSC guidance.
- **Multi-Factor Authentication (MFA):** St. Mark's Catholic Primary School will implement MFA where feasible, prioritising access to sensitive systems such as MIS, remote access, and email.

Device Security

To protect school-issued devices and data, users are required to:

- Screen Lock devices left unattended.
- Update operating systems and applications on devices when prompted.
- Report lost or stolen equipment immediately to IT Support.
- Change all account passwords if a device is lost or stolen and notify IT Support.
- Report any suspected threats or security weaknesses to the Risk Register Owner.

Device Configuration: Devices will include the following security controls as a minimum:

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

BYOD: Staff personal devices used to access school systems must adhere to security policies, including password protection, anti-virus, and encryption where possible. Where the Head approves the use of personal devices, your support provider can do the technical checks and add devices to the network. Periodic spot checks will be undertaken to ensure compliance with this requirement.

Data Security

St. Mark's Catholic Primary School will implement robust measures to protect data confidentiality, integrity, and availability, in line with the school's GDPR policy.

Confidential Data Definition: Confidential data includes:

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

Data Retention: Data will be retained only as necessary for school operations, per UK-GDPR regulations.

Backups: Critical data and systems will be backed up according to the 3-2-1 backup methodology:

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

Data Encryption: Encryption will be applied to all stored confidential data, both in transit and at rest, to enhance protection against unauthorised access.

Sharing Files

St. Mark's Catholic Primary School recognises the risks associated with sharing confidential data and requires users to:

- Be wary of emails that are in any way suspicious, request urgent or time limited actions
- Verify emails for potential phishing or suspicious activity before clicking on any links, opening any attachments or responding,
- Verify any requests for or changes to financial information with known contact details for the sender, not by replying to the email or using any contact details contained within it.
- Store files only on school-managed systems. Do not send school files to personal accounts
- Verify data recipients before sending. Before sharing any confidential or sensitive data, users must take steps to ensure the recipient is legitimate and authorised to receive information.
- Use encryption when sending any confidential information.
- Alert IT Support / data protection to any suspected breaches, scams, or malicious activity immediately. Remember data breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours

Training

St. Mark's Catholic Primary School will conduct regular cybersecurity training, providing additional training to staff responsible for IT maintenance. Phishing simulations will also be conducted to help staff recognise and respond to threats.

Training is available to all school staff via the National Cyber Security Centre.

System Security
Security will be built into IT service design at St. Mark's Catholic Primary School through the following:

- **Security Patching**: All network hardware, operating systems, and software will be kept updated.
- **Lifecycle Management**: Regular assessment and proactive planning for the replacement of systems and software before security support ends.
- **Anti-Virus Management**: Anti-virus systems will be actively managed and monitored.
- **Backup Testing**: Backups will be tested regularly to ensure data recoverability.
- **Security Audits and Vulnerability Scanning**: Regular audits and scans will be conducted to detect and remediate risks.
- **Network Segmentation**: Visitor devices will connect via a separate wireless network from critical school systems.
- **Access Control**: Access to systems is based on the principle of least privilege, providing users only with permissions necessary for their role.

Major Incident Response Plan
St. Mark's Catholic Primary School will develop, maintain, and test a Cybersecurity Major Incident Response Plan that includes:

- Identification of key decision-makers
- Prioritisation of system and backup restoration based on school needs
- Emergency plans for school functionality without digital access
- Alternative communication methods and emergency contact lists
- Allocated emergency budgets and access processes
- Contact details for key support agencies, such as IT support providers

Following an incident, a post-incident review will be conducted to update response protocols and strengthen defences.

Budget and Security Investment
St. Mark's Catholic Primary School recognises that the cost of recovering from a major cybersecurity incident can greatly exceed ongoing investment in secure IT. Therefore, St. Mark's Catholic Primary School will allocate budget resources to support regular updates, maintenance, and improvements to reduce cyber risk.

Policy Review
This policy will be reviewed annually or in response to significant regulatory or technological changes, with updates approved by the Governing Board.