



St Michael & St Martin Catholic Primary School

Cyber Security Policy and Incident Response Plan

Purpose and scope

This policy protects teaching, safeguarding, school operations and information against cyber threats. It covers devices, accounts, networks, cloud services, suppliers and authorised remote access. The school implements proportionate controls, checks their effectiveness and maintains a practical response and recovery plan.

Responsibilities

- The Governing Board oversees cyber risk, resources and recovery readiness. The Headteacher leads school incident decisions and continuity arrangements.
- The SLT digital lead maintains the asset and risk registers, coordinates IT support and reports assurance and outstanding risks to leaders.
- IT support implements agreed controls, reports gaps, maintains recovery documentation and provides technical incident response. Outsourcing does not remove school accountability.
- The DPO advises on personal data risks, breach assessment and reporting. The DSL handles any linked risk to children.
- All users follow acceptable use rules, complete training and report incidents immediately.

Risk management and procurement

Maintain an inventory of devices, software, cloud services, owners, support status and critical functions. Record risks and remediation owners. Before introducing a service, assess security, access, supplier support, safeguarding, privacy, backups, contractual responsibilities and exit arrangements. Unsupported systems must be replaced or isolated with a documented risk decision.

Training and assurance

Provide induction and at least annual cyber security awareness training, with additional updates when risks change. Training includes phishing, authentication, secure information handling and reporting. Review security controls, access and recovery arrangements at least annually and after significant incidents. Governors receive an assurance report that protects sensitive security details.

Preventive controls

Accounts and access

- Give users unique accounts with the minimum permissions needed. Separate administrative accounts from routine work and restrict privileged access.
- Use strong unique passwords, secure recovery arrangements and multi-factor authentication for privileged, remote and cloud access in line with DfE standards and risk assessment.
- Apply documented joiner, mover and leaver procedures. Remove access promptly when no longer needed; review privileged, shared and supplier access regularly.
- Use time-limited supplier access where practicable and retain an audit trail. Do not publish credentials or include passwords in this policy.

Devices networks and software

- Maintain supported software, security updates, endpoint protection, firewalls and secure configurations. Apply urgent fixes promptly in accordance with provider advice and DfE standards.
- Encrypt portable equipment containing personal or confidential data and enable appropriate lock, recovery and remote management arrangements.
- Separate guest access from school information systems and use network segmentation proportionate to risk. Secure wireless and remote access.
- Restrict software installation and removable storage. Log relevant security activity, protect logs and investigate significant alerts.
- Verify requests for bank-detail changes, payments or sensitive information independently. Use finance approval controls even where a message appears to come from a senior leader.

Backups and continuity

Back up critical information and configurations using protected arrangements that include a copy isolated from routine accounts and ransomware risk. Cloud synchronisation alone is not a sufficient recovery strategy. Agree backup frequency, retention, recovery time and acceptable data loss for each critical service, and document responsibility.

Test restoration at least annually and after significant changes, recording results and actions. Keep an accessible offline copy of incident contacts and essential continuity instructions. Plan how to maintain pupil safety, attendance, emergency contacts, medication and safeguarding access during an outage without creating insecure substitute systems.

Incident response plan

Use this plan for suspected phishing compromise, malware, ransomware, unauthorised access, stolen devices, service disruption or data loss. Start promptly; uncertainty is not a reason to delay reporting.

Stage	Action and responsibility
1 Report immediately	User stops risky activity and contacts IT support and the Headteacher through a trusted route. Use telephone if email may be compromised. Inform the DSL if children may be at risk and the DPO if personal data may be affected.
2 Contain safely	IT support isolates affected equipment or accounts and blocks further access. Do not delete, reset, reinstall or power down equipment unless advised. Preserve logs and evidence. Record the time the school became aware.
3 Assess and coordinate	Headteacher appoints an incident lead. IT assesses scope, entry route and affected services. DPO assesses personal data risk; DSL assesses safeguarding impact. Open an incident log and agree safe communications.
4 Maintain essential services	Headteacher activates business continuity arrangements. Use verified offline records and authorised alternatives; communicate with staff and families as necessary without disclosing sensitive incident details.
5 Notify where required	DPO advises on ICO reporting and affected individuals. Headteacher considers insurer or RPA conditions, police, DfE and other relevant reporting. Do not wait for a full investigation where a deadline applies.
6 Recover and review	IT removes the cause, verifies clean systems, restores tested backups and resets credentials as required. Headteacher authorises resumption after assurance. Record lessons, actions, owners and completion dates.

Important response rules

Do not contact attackers, negotiate or pay a ransom independently. Refer any extortion demand immediately to the incident lead, police and insurer or RPA adviser. Do not send confidential information through compromised channels. Maintain a factual log of decisions, evidence and communications.

A cyber incident may also be a personal data breach. Where notification is required, the school reports to the ICO without undue delay and within 72 hours of awareness. If information is incomplete, an initial notification can be followed by updates. The Data Protection Policy sets out the assessment and recording procedure.

Contacts records and recovery assurance

Complete before approval and hold an offline copy

Contact or arrangement	Details
School incident lead and deputy	Nicola Duggan/Sabina Bell
IT provider and emergency response	Infologix IT Services Ltd. 0208 133 3374
DPO and deputy contact	Judicium (details on website)
DSL and deputy route	Nicola Duggan/Sabina Bell
Chair of Governors	Remie Antao
Insurer or RPA reporting requirements	Diocesan Insurance
Protected backups and last restore test	Infologix IT Services Ltd.
External reporting routes	ICO breach reporting; police 999 for immediate danger or 101 as appropriate; NCSC incident reporting; relevant DfE and insurer or RPA routes

Incident log fields

Record incident reference; reporting person; awareness date and time; affected assets and services; suspected cause; containment; safeguarding and data protection assessments; notifications and reasons; evidence location; communications; recovery checks; authorisation to resume; and corrective actions with owners and dates. Restrict the log to authorised staff.

Review and sign off

After an incident, review whether access controls, updates, supplier arrangements, backups, training or continuity plans need to change. Report material risks and actions to governors without unnecessary personal information or security detail.

Guidance and related documents

DfE cyber security standard

ICO personal data breach guidance

Read alongside the school Child Protection and Safeguarding Policy, Staff Code of Conduct, Behaviour Policy, Mobile Phone Policy and the other school IT policies. Guidance checked September 2026.