St John Fisher Catholic Primary School
Cyber Security Policy
2026-2028

1. Policy Statement

St John Fisher is committed to maintaining robust cyber security practices to protect its systems, data, learners, staff, and stakeholders. The school recognises cyber security as a safeguarding and data protection priority.

This policy aligns with:

- Department for Education Cyber Security Standards for Schools and Colleges
- National Cyber Security Centre (NCSC) guidance for education
- Keeping Children Safe in Education (KCSIE)
- Information Commissioner's Office (ICO) UK GDPR guidance
- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018

2. Policy Objectives

This policy aims to:

- Protect school systems and data from cyber threats
- Ensure confidentiality, integrity, and availability of information systems
- Reduce the risk of data breaches and safeguarding incidents
- Ensure compliance with statutory safeguarding and data protection duties
- Promote safe and responsible digital use across the school community

3. Scope

This policy applies to:

- All staff (teaching and non-teaching)
- Governors
- External IT providers and contractors
- Pupils accessing school systems or devices

- Any personal or school-owned devices used to access school data

4. Governance and Responsibilities

4.1 Governing Body

The Governing Body is responsible for:

- Ensuring cyber security risk is effectively managed
- Receiving termly reports on cyber security status
- Ensuring adequate resources are in place

4.2 Headteacher / Senior Leadership Team

Responsible for:

- Overall implementation of this policy
- Ensuring staff compliance
- Ensuring risks are escalated appropriately

4.3 Data Protection Officer (DPO)

Responsible for:

- Monitoring UK GDPR compliance
- Advising on data breach management
- Overseeing Data Protection Impact Assessments (DPIAs)

4.4 IT Provider / IT Lead

Responsible for:

- Implementing technical controls
- Monitoring security systems
- Managing updates, patches, and backups
- Supporting incident response procedures

4.5 All Staff

Responsible for:

- Following safe cyber security practices
- Reporting suspicious activity or incidents immediately
- Completing mandatory training

5. Cyber Security Controls

The school maintains the following minimum controls:

- Multi-factor authentication (MFA) for staff and administrative accounts
- Regular patching and system updates
- Endpoint protection (anti-virus/EDR)
- Secure backups (including offline or immutable storage)
- Role-based access controls and least privilege principles
- Filtering and monitoring systems for safeguarding compliance

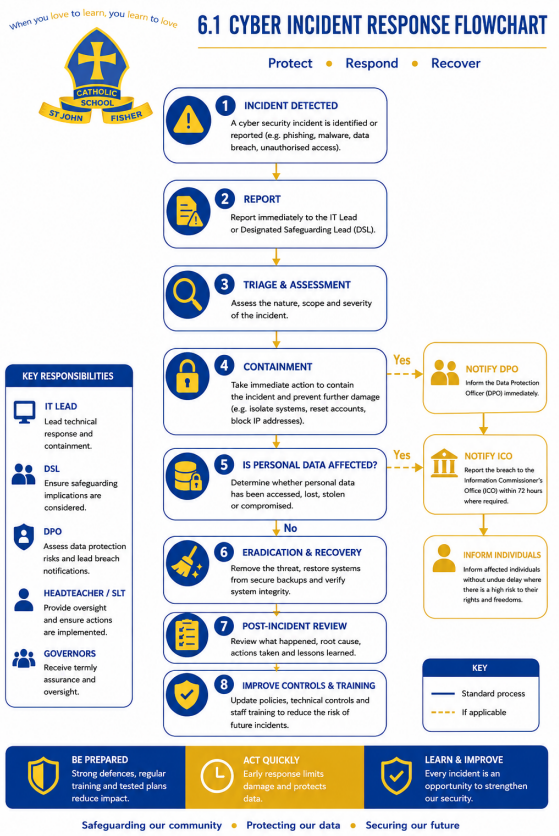
6. Incident Management

All cyber security incidents must be reported immediately to the IT Lead and/or DSL.

Incidents include:

- Suspected phishing or malicious emails
- Data breaches or loss of personal data
- Unauthorized access to systems
- Ransomware or malware attacks

6.1 Cyber Incident Response Flowchart



6.2 Incident Management Process

- All incidents are logged by the IT Lead
- Severity is assessed based on safeguarding, data type, and operational impact
- Immediate containment is prioritised
- Recovery is completed using secure systems and verified backups
- All significant incidents require a formal post-incident review

7. Data Protection and GDPR

The school complies with UK GDPR principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

DPIAs are completed for high-risk processing activities.

8. Safeguarding and Online Safety

Cyber security is integral to safeguarding practice.

- Filtering and monitoring systems are in place
- Safeguarding platforms are securely configured
- Online safety training is provided to staff annually

9. Training and Awareness

- Annual cyber security and GDPR training for staff
- Induction training for new staff
- Regular awareness updates on emerging threats

10. Monitoring and Review

- Reviewed annually or following a cyber incident
- Monitored termly through governor reporting
- Updated in line with DfE, NCSC, or ICO guidance

11. Breach Notification

Where a personal data breach occurs:

- Risk to individuals is assessed
- ICO is notified within 72 hours where required
- Affected individuals are informed where necessary
- All actions are documented

12. Related Documents

- Appendix A: Cyber Security Self-Assessment Checklist
- Appendix C: Accessibility Plan
- Safeguarding Policy
- Data Protection Policy
- Acceptable Use Policy

When you love to learn, you learn to love

CATHOLIC SCHOOL ST JOHN FISHER

6.1 CYBER INCIDENT RESPONSE FLOWCHART

Protect • Respond • Recover

1 INCIDENT DETECTED
A cyber security incident is identified or reported (e.g. phishing, malware, data breach, unauthorised access).

2 REPORT
Report immediately to the IT Lead or Designated Safeguarding Lead (DSL).

3 TRIAGE & ASSESSMENT
Assess the nature, scope and severity of the incident.

4 CONTAINMENT
Take immediate action to contain the incident and prevent further damage (e.g. isolate systems, reset accounts, block IP addresses).

Yes → **NOTIFY DPO**
Inform the Data Protection Officer (DPO) immediately.

5 IS PERSONAL DATA AFFECTED?
Determine whether personal data has been accessed, lost, stolen or compromised.

Yes → **NOTIFY ICO**
Report the breach to the Information Commissioner's Office (ICO) within 72 hours where required.

INFORM INDIVIDUALS
Inform affected individuals without undue delay where there is a high risk to their rights and freedoms.

No

6 ERADICATION & RECOVERY
Remove the threat, restore systems from secure backups and verify system integrity.

7 POST-INCIDENT REVIEW
Review what happened, root cause, actions taken and lessons learned.

8 IMPROVE CONTROLS & TRAINING
Update policies, technical controls and staff training to reduce the risk of future incidents.

KEY RESPONSIBILITIES

IT LEAD
Lead technical response and containment.

DSL
Ensure safeguarding implications are considered.

DPO
Assess data protection risks and lead breach notifications.

HEADTEACHER / SLT
Provide oversight and ensure actions are implemented.

GOVERNORS
Receive termly assurance and oversight.

KEY

— Standard process

---- If applicable

BE PREPARED
Strong defences, regular training and tested plans reduce impact.

ACT QUICKLY
Early response limits damage and protects data.

LEARN & IMPROVE
Every incident is an opportunity to strengthen our security.

Safeguarding our community • Protecting our data • Securing our future