St Joseph's Primary School
Cyber Security Policy

Purpose

This policy sets out how the school prevents, detects, responds to and recovers from cyber threats. It supports the school's duty of care to protect users and data and aligns with the Education Digital Standards, Cyber response plan for schools, National Cyber Security Centre (NCSC) guidance and NCSC Cyber Essentials

Scope

This policy applies to:

- Cyber threats including phishing, ransomware, malware and unauthorised access
- Staff, learners and governors
- Suppliers of third-party services and solutions
- Technical systems and cloud services
- Incident response and business continuity

Policy Statement

The school will take a proactive, risk-based approach to cyber security to:

- Reduce the likelihood and impact of cyber incidents
- Ensure timely and effective response to threats
- Build awareness and resilience across the school community

Cyber Security Strategy

The school will maintain a cyber security strategy that:

- Is supported by senior leaders and governors
- Is informed by risk assessment and incident learning
- Is reviewed regularly in line with emerging threats
- Is inclusive of all services and solutions, including those from third-party suppliers

Supplier Management

The school will ensure that suppliers:

- Can demonstrate adherence to school policy and alignment with the Education digital standards and the Cyber response plan for schools,
- Are familiar with school incident response plan and able to respond effectively

Awareness and Education

The school will ensure that:

- Staff receive regular cyber-security training covering phishing, credential theft, malicious links, social engineering, ransomware, AI-enabled scams and other emerging threats.

© SWGfL 2026

- Learners receive age-appropriate education about cyber security, scams, account protection and the lawful and responsible use of systems.
- Governors understand their oversight responsibilities

Incident Response

The school will maintain a clear cyber incident response plan that:

- Defines roles and escalation routes
- Supported by an effective communications strategy
- Supports safeguarding and business continuity
- uses cyber incident exercises periodically to test preparedness and identify improvements.
- Ensures incidents are recorded and reviewed
- identifies responsibilities for safeguarding, technical response, communications, data protection and external reporting.

External Assurance

Where appropriate, the school will engage external expertise to assess cyber resilience and will work towards recognised standards or certifications.

Review

Cyber security arrangements will be reviewed annually, or sooner if required by incidents, guidance or changes in technology. Lessons learned from managing incidents should inform improvements to the strategy.

© SWGfL 2026