Date of last review: n/a
Date of next review: June 2027

CYBER SECURITY POLICY

Table of contents

1. 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 DfE Cyber Security Standards, National Cyber Security Centre (NCSC guidance and NCSC Cyber Essentials.

2. Scope

This policy applies to:

- Cyber threats including phishing, ransomeware, 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

3. 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

4. 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

5. Supplier Management

The school will ensure that suppliers:

- Can demonstrate adherence to school policy and alignment with the DfE Cyber Security Standards
- Are familiar with the school **Critical Incident Plan** and able to respond effectively

6. Awareness and Education

The school will ensure that:

- Staff receive regular cyber awareness training
- Learners receive age-appropriate education on cyber risks
- Governors understand their oversight responsibilities

7. 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
- Is tested periodically through simulations or exercises
- Ensures incidents are recorded and reviewed

8. External Assurance

The school will engage external expertise (Bloobo) to assess cyber resilience and will work towards recognized standards or certifications.

9. 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.

10. Related School Policies and Procedures

This policy will be implemented in conjunction with the following school policies:

- **Online Safety Policy**

- **Technical Security Policy**
- **Data Protection Policy**
- **Safeguarding Policy**
- **Critical Incident Plan**

Version control table

Version	Date	Changes	Approval
1	2026	New policy.	SO