Date of last review: N/A
Date of next review: June 2027

TECHNICAL SECURITY POLICY
(INCLUDING ACCESS, DEVICE AND INCIDENT MANAGEMENT)

Table of contents

1. Purpose

This policy sets out how the school protects its technical infrastructure, systems and devices to ensure a secure and resilient digital environment. It supports safeguarding, data protection and business continuity and aligns with the DfE Technical Standards.

2. Scope

This policy applies to:

- Staff, learners and governors
- Suppliers of third-party services and solutions
- School networks, servers and cloud systems
- School-owned devices
- User accounts and access controls
- Device configuration and management, including personal devices where permitted

3. Policy Statement

The school will ensure that its technical systems are managed in a way that:

- Protects users and data from unauthorised access or misuse
- Supports safe and reliable access to digital services

- Enables detection, response and recovery from technical incidents
- Is proportionate to risk and regularly reviewed

4. Access Control and Authentication

The school will ensure that:

- All users have unique accounts with appropriate access rights
- New user rights are allocated as part of induction
- Access is removed promptly when users leave the school
- Passwords and authentication methods reflect NCSC and DfE guidance
- Multi-factor authentication is used for sensitive systems where appropriate
- Administrator access is restricted and monitored
- System administrators and those with global/confidential data system access use a physical security device in addition to MFA to access systems.

5. System Security and Maintenance

The school will ensure that:

- Systems and software are licensed, supported and kept up to date
- Security patches are applied promptly
- Anti-virus and malware protection is in place across all systems
- Backups are taken regularly and stored securely
- Physical access to infrastructure is controlled

6. Device Management

The school will ensure that:

- Clear expectations exist for the use of school-owned and personal devices
- School devices are configured securely and managed appropriately, with regular automatic patches and updates
- Where personal devices are permitted, expectations are clearly defined and risk-assessed
- Acceptable Use Agreements reference responsible device use
- Users receive guidance on safe and appropriate device use

7. Supplier Management

The school will ensure that:

- Provision of third-party services and solutions are adequately contracted and regularly reviewed
- Suppliers can demonstrate adherence to school policy and alignment with the DfE Technical Standards

8. Incident Management

Technical incidents will be logged, escalated and reviewed. Serious incidents will be managed in line with safeguarding and business continuity procedures.

9. Review and Training

Technical security arrangements will be reviewed regularly. This is a non-statutory policy and will be reviewed bi-annually or sooner if required by incidents, guidance or changes in technology. Staff with specific responsibilities will receive appropriate training, and users will be educated on their responsibilities.

10. Related School Policies and Procedures

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

- **Online Safety Policy**
- **Cyber Security Policy**
- **Safeguarding Policy**
- **Data Protection Policy**
- **Critical Incident Plan**

Version control table

Version	Date	Changes	Approval
1	2026	New policy.	SO