Pennington C of E Primary School
BeTheBestYouCanBe!

CYBER SECURITY POLICY

2026-27

PENNINGTON C OF E PRIMARY SCHOOL

Pennington C of E Primary School
BeTheBestYouCanBe!

Cyber Security Policy

Item	Detail
Policy Owner	Headteacher
Approved By	Governing Board
Review Frequency	Annually
Date Approved	September 2026
Review Date	September 2027

1. Policy Statement

Pennington Church of England Primary School recognises that effective cyber security is essential to protect pupils, staff, governors, volunteers, visitors and the school community.

The school is committed to safeguarding personal data, maintaining the integrity of its information systems and ensuring the continuity of education and business operations.

This policy sets out the school's approach to reducing cyber security risks and responding to incidents in a timely and effective manner.

2. Scope

This policy applies to:

- All staff
- Governors
- Volunteers
- Contractors
- Visitors using school systems
- Any individual accessing school information or networks

The policy covers:

- School-owned devices
- Personal devices used for school business
- Cloud-based services
- Email systems
- Wi-Fi and network infrastructure
- Data stored electronically

3. Key Principles

The school will:

- Protect confidential information from unauthorised access.
- Maintain secure systems and devices.
- Promote good cyber security awareness amongst all users.
- Comply with UK GDPR and the Data Protection Act 2018.
- Report and respond promptly to cyber incidents.
- Follow relevant DfE cyber security guidance for schools.

4. Roles and Responsibilities

Governing Board

The Governing Board will:

- Monitor cyber security risks.
- Ensure appropriate policies are in place.
- Receive reports on significant incidents.

Headteacher

The Headteacher is responsible for:

- Ensuring implementation of this policy.
- Promoting a culture of cyber awareness.
- Escalating significant incidents to governors and relevant authorities.

Staff

All staff must:

- Follow this policy.
- Complete any required cyber security training.
- Protect passwords and authentication methods.
- Report suspected cyber incidents immediately.

5. Password Requirements

Users must:

- Create strong passwords.
- Avoid sharing passwords with others.
- Use unique passwords for school systems where possible.
- Change passwords immediately if compromise is suspected.

Passwords must never be:

- Written on display
- Shared by email
- Shared with colleagues

6. Multi-Factor Authentication (MFA)

Where available, staff must use MFA to provide additional protection against unauthorised access.

MFA is currently expected for services including:

- Microsoft 365
- Administrative systems where supported
- Third-party services containing personal data – e.g. CPOMS

Failure to follow MFA requirements may result in access restrictions.

7. Email Security

Staff should:

- Be cautious of unexpected emails.
- Verify requests involving money, personal data or passwords.
- Report phishing attempts immediately.
- Never click suspicious links or open unexpected attachments.

Common warning signs include:

- Urgent requests for action
- Requests for payment
- Requests for login credentials
- Poor spelling or unusual email addresses

8. Device Security

School devices must:

- Be password protected.
- Receive security updates promptly.
- Use approved anti-malware software where required.
- Be locked when unattended.

Lost or stolen devices must be reported immediately.

9. Personal Devices

Where personal devices are used for school business:

- Appropriate security settings must be applied.
- Devices must be password protected.
- School data must not be downloaded unnecessarily.
- School information must not be stored indefinitely on personal devices.

The school reserves the right to withdraw permission for the use of personal devices where security concerns arise.

10. Data Protection

Users must:

- Access only information required for their role.
- Store personal data securely.
- Follow the school's Data Protection Policy.
- Report any suspected data breach immediately.

Particular care must be taken when handling:

- Safeguarding records
- SEND information
- Health information
- Personnel records
- Pupil data

11. Software and Applications

Only authorised software and applications may be used for school business.

Staff must not:

- Install unauthorised software.
- Circumvent security controls.
- Upload sensitive information to unapproved systems.

New applications handling personal data must be approved through the school's data protection processes.

12. Backups and Business Continuity

The school will ensure that critical systems are appropriately backed up through approved providers and services.

The school will maintain arrangements to support recovery from:

- Cyber attacks
- Data loss
- System failures
- Ransomware incidents

13. Incident Reporting

All suspected cyber security incidents must be reported immediately to the Headteacher and relevant IT support provider.

Examples include:

- Phishing emails
- Malware infections
- Lost devices
- Unauthorised access
- Suspected data breaches
- Compromised passwords

Where required, incidents will also be reported to:

- Data Protection Officer
- Hampshire County Council (where appropriate)
- Information Commissioner's Office (ICO)
- Department for Education
- National Cyber Security Centre (NCSC)

14. Training and Awareness

The school will provide regular opportunities for staff to develop cyber security awareness.

This may include:

- Annual staff briefings
- Phishing awareness training
- Data protection updates
- Safeguarding-linked cyber security training

15. Monitoring and Review

Compliance with this policy will be monitored by the Headteacher and Governing Board.

The policy will be reviewed annually or sooner if:

- Significant changes occur in technology.

- New threats emerge.
- Guidance from government agencies changes.
- A major incident occurs.

Linked Policies

- Safeguarding and Child Protection Policy
- Data Protection Policy
- Staff Code of Conduct
- Online Safety Policy
- Acceptable Use Agreement
- Remote Learning Policy
- Business Continuity Plan

Governor Addition

The Governing Board recognises cyber security as a significant strategic risk and will receive annual assurance regarding compliance, staff training, cyber incidents and the effectiveness of security controls.