

NORTON COMMUNITY PRIMARY SCHOOL

Cyber Security Policy 2026 2027

Nothing is beyond our reach!

Policy Information

Item	Details
Policy Name	Cyber Security Policy
Policy Owner	Headteacher
Approved By	Governing Board
Date Approved	Autumn 2026
Review Date	Autumn 2027

Vision Statement

Nothing is beyond our reach!
Care and challenge engage and motivate us!
Praise reassures and supports us!
Successes are celebrated and built on!

At Norton Community Primary School we are committed to providing a caring, safe, inclusive and respectful environment where every child feels valued and able to achieve their full potential.

1. Policy Statement

Norton Community Primary School recognises that cyber security is essential to protecting children, staff, school data and educational provision.

The school is committed to maintaining secure systems, promoting responsible use of technology and reducing cyber risks through effective governance, technical controls and staff awareness. This reflects DfE expectations that schools implement appropriate cyber security measures and procedures.

2. Scope

This policy applies to:

- Employees
- Governors
- Volunteers
- Contractors

- Visitors using school systems
- Third-party providers

It covers:

- School devices
- School networks
- Cloud systems
- Email systems
- School-owned data

3. Cyber Security Principles

The school will:

Protect

Protect systems and information from unauthorised access.

Detect

Monitor for threats and unusual activity.

Respond

Deal promptly with cyber incidents.

Recover

Restore services safely and quickly.

4. Acceptable Use

Users must:

- Use school systems professionally.
- Keep passwords secure.
- Lock devices when unattended.
- Report suspicious activity immediately.

Users must not:

- Share passwords.
- Download unauthorised software.
- Circumvent security controls.
- Access inappropriate websites.
- Use personal devices to store confidential school information unless authorised.

5. Password Requirements

Passwords must:

- Be unique.
- Be kept confidential.
- Not be shared.

Where available:

- Multi-factor authentication should be used.

Users must immediately report suspected credential compromise.

6. Email Security

Staff must:

- Be vigilant for phishing emails.
- Verify unexpected financial requests.
- Exercise caution with attachments and links.

Staff must not:

- Open suspicious attachments.
- Share confidential data without authorisation.

7. Device Security

All school devices will:

- Use anti-malware protection.
- Receive regular updates.
- Be appropriately configured.
- Be protected by passwords.

Loss or theft of devices must be reported immediately.

8. Data Security

The school will:

- Restrict access according to job role.
- Protect confidential information.
- Securely dispose of data.
- Maintain appropriate backups.

Staff will only access information required for their role.

9. Filtering and Monitoring

The school will maintain internet filtering and monitoring arrangements to support safeguarding and reduce cyber risks. Staff and pupils are expected to comply with these arrangements. This aligns with KCSIE requirements regarding online safety and filtering and monitoring systems.

10. Artificial Intelligence

The use of AI tools must:

- Comply with data protection legislation.
- Protect confidential information.
- Support rather than replace professional judgement.

Staff must not input personally identifiable pupil information into public AI systems unless approved and appropriately safeguarded.

11. Staff Training

The school will provide:

- Cyber awareness training at induction.
- Annual refresher training.
- Updates in response to emerging threats.

Training will include:

- Phishing awareness
- Password security
- Online safety
- Data protection
- Cyber incident reporting

12. Governance and Monitoring

The Governing Body will:

- Review cyber risks annually.
- Monitor significant incidents.
- Support ongoing cyber resilience improvements.

The Business Manager will conduct an annual review of this policy and oversee implementation.