

# Cyber Attack and Cyber Incident Response Policy 2026 2027

*Nothing is beyond our reach!*

## Policy Information

| Item          | Details                                         |
|---------------|-------------------------------------------------|
| Policy Name   | Cyber Attack and Cyber Incident Response Policy |
| Policy Lead   | 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 is committed to protecting its pupils, staff, governors, volunteers, contractors, and visitors from cyber threats and cybersecurity incidents.

The school recognises that cyber attacks can have significant impacts on safeguarding, teaching and learning, school operations, finances, reputation, and compliance with data protection legislation. The school will take all reasonable steps to prevent, detect, respond to, and recover from cyber security incidents.

This policy applies to all users of school systems, devices, networks and data.

## 2. Legal and Regulatory Framework

This policy should be read alongside:

- UK General Data Protection Regulation (UK GDPR)

- Data Protection Act 2018
- Computer Misuse Act 1990
- Keeping Children Safe in Education (2026)
- Prevent Duty Guidance
- DfE Cyber Security Standards for Schools and Colleges
- DfE Filtering and Monitoring Standards
- North Yorkshire Council ICT and Information Governance requirements
- School Data Protection Policy
- School Acceptable Use Policies
- School Safeguarding and Child Protection Policy

The school has a statutory responsibility to safeguard children online and offline and to implement appropriate cyber security measures to protect pupils, staff, and information systems.

### **3. Definition of a Cyber Attack**

A cyber attack is any deliberate attempt to gain unauthorised access to, disrupt, damage, alter, steal, or destroy information systems, networks, devices, or data.

Examples include:

- Phishing emails
- Malware infections
- Ransomware attacks
- Data breaches
- Account compromise
- Identity theft
- Unauthorised access to school systems
- Denial of Service (DoS) attacks
- Theft of devices containing school data
- Malicious use of Artificial Intelligence tools
- Insider cyber threats

### **4. Responsibilities**

#### **Governing Body**

The Governing Body will:

- Ensure appropriate cyber security arrangements are in place.

- Monitor cyber risks through regular reports.
- Ensure this policy is reviewed annually.
- Support appropriate investment in cyber security controls.

### **Headteacher**

The Headteacher will:

- Lead the strategic response to significant cyber incidents.
- Authorise emergency actions where needed.
- Inform governors of significant incidents.

### **Business Manager**

The Business Manager will:

- Coordinate cyber security arrangements.
- Maintain this policy.
- Liaise with IT providers and North Yorkshire Council where required.
- Coordinate incident reporting.
- Ensure cyber security training is delivered.

### **ICT Provider / Technical Support**

The school's ICT provider will:

- Maintain security updates.
- Operate anti-malware solutions.
- Monitor threats and vulnerabilities.
- Maintain backup systems.
- Support incident investigation and recovery.

### **All Staff**

All staff must:

- Follow school cyber security procedures.
- Use strong passwords.
- Protect confidential information.
- Report suspected incidents immediately.
- Complete required cyber security training.

Failure to comply may result in disciplinary action.

## **5. Cyber Security Controls**

The school will maintain appropriate security arrangements, including:

### **Access Controls**

- Individual user accounts only.
- Strong password requirements.
- Multi-factor authentication where available.
- Removal of accounts when staff leave.

### **Device Security**

- Anti-malware protection.
- Security updates and patching.
- Encrypted devices where appropriate.
- Screen locking after periods of inactivity.

### **Network Security**

- Managed firewall protection.
- Secure Wi-Fi arrangements.
- Filtering and monitoring systems.
- Restricted administrator privileges.

### **Data Protection**

- Secure storage of sensitive information.
- Restricted access based on role.
- Secure disposal of records.
- Encryption of confidential information where appropriate.

### **Backups**

The school will maintain:

- Regular backups of critical systems.
- Secure off-site or cloud-based backups.
- Periodic testing of backup restoration.

These controls reflect DfE cyber security expectations for schools.

## **6. Staff Awareness and Training**

The school will:

- Provide cyber security awareness training for all staff.
- Deliver annual refresher training.
- Raise awareness of:
  - phishing attacks
  - ransomware
  - password security
  - safeguarding implications
  - safe use of AI technologies
  - data protection responsibilities

New staff will receive cyber security information during induction.

## **7. Reporting a Suspected Cyber Incident**

Any member of staff who suspects a cyber incident must report it immediately to:

1. The Business Manager.
2. The Headteacher.
3. ICT Support Provider.

Staff must not:

- Attempt their own investigation.
- Delete evidence.
- Reset affected devices unless instructed.

Examples requiring immediate reporting include:

- Suspicious emails opened accidentally.
- Unexpected password changes.
- Missing devices.
- Malware alerts.
- Unauthorised access to school data.
- Ransomware messages.

## **8. Cyber Incident Response Procedure**

### **Phase 1 – Identify**

The school will:

- Determine the nature of the incident.

- Identify affected systems.
- Assess safeguarding risks.
- Assess whether personal data may have been compromised.

### **Phase 2 – Contain**

The school may:

- Disconnect affected devices.
- Disable user accounts.
- Block malicious activity.
- Isolate parts of the network.

### **Phase 3 – Escalate**

Where appropriate the school will notify:

- ICT support provider.
- North Yorkshire Council.
- Governing Body.
- Data Protection Officer.
- Information Commissioner's Office (ICO).
- Police.
- National Cyber Security Centre (NCSC).

### **Phase 4 – Recover**

The school will:

- Restore systems from backups where appropriate.
- Verify systems are secure.
- Resume services safely.
- Monitor for recurring activity.

### **Phase 5 – Review**

Following any significant incident:

- A lessons learned review will be completed.
- Actions will be incorporated into improvement plans.
- Governors will receive a summary report.

## **9. Data Breaches**

Where personal data is compromised, the school will follow its Data Protection Policy and breach procedures.

The school will assess:

- Nature of information involved.
- Potential harm to individuals.
- Safeguarding implications.
- Whether ICO reporting requirements apply.

Any notifiable breach will be reported within required statutory timescales.

### **10. Communication During a Cyber Incident**

The Headteacher will determine communications required.

Communications may include:

- Staff briefings.
- Parent communications.
- Governor updates.
- Local Authority notifications.
- Regulatory reporting.

Only authorised staff may communicate externally regarding a cyber incident.

### **11. Business Continuity**

The school will maintain arrangements to continue essential operations where systems become unavailable.

This may include:

- Paper attendance registers.
- Paper safeguarding records (where necessary).
- Alternative communication methods.
- Manual finance and administrative procedures.

### **12. Monitoring and Review**

The school will:

- Conduct an annual cyber risk assessment.
- Review cyber risks termly.
- Review this policy annually.
- Review the policy following any significant cyber incident.

These actions align with current DfE cyber security standards for schools.

#### **Appendix A – Immediate Action Checklist**

If a cyber attack is suspected:

- ✓ Stop using the affected device
- ✓ Disconnect from the network if instructed
- ✓ Inform the Business Manager immediately
- ✓ Inform the Headteacher immediately
- ✓ Contact ICT support provider
- ✓ Preserve evidence
- ✓ Record actions taken
- ✓ Follow instructions from incident lead

This policy has been developed for Norton Community Primary School and aligns with the school's safeguarding framework and current DfE cyber security expectations