

Cyber Incident Response Plan 2026 2027

Nothing is beyond our reach!

Policy Information

Item	Details
Policy Name	Cyber Incident Response Plan
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. Purpose

The purpose of this plan is to ensure that Norton Community Primary School can respond quickly and effectively to cyber incidents in order to:

- Protect children and staff.
- Minimise disruption to education.
- Protect personal data.
- Restore critical systems safely.
- Meet statutory and regulatory requirements.

Cyber incidents may present safeguarding risks if confidential pupil information is compromised. Cyber incident management therefore forms part of the school's safeguarding arrangements.

2. Incident Response Team

Role	Responsibility
Headteacher	Overall incident lead
Business Manager	Incident Coordinator
ICT Support Provider	Technical response
Data Protection Officer	Data breach assessment
Chair of Governors	Strategic oversight
Designated Safeguarding Lead	Safeguarding risk assessment

3. Cyber Incident Severity Levels

Level 1 – Minor

Examples:

- Suspicious email received
- Single device malware alert
- User account lockout

Impact:

- No significant disruption
- No data loss

Response:

- Report to ICT support
- Monitor and resolve

Level 2 – Significant

Examples:

- Staff account compromised
- Potential data breach
- Multiple infected devices

Impact:

- Limited disruption
- Possible personal data exposure

Response:

- Incident team activated
- DPO consulted
- Investigation commenced

Level 3 – Critical

Examples:

- Ransomware attack
- Major system outage
- Large-scale data breach

Impact:

- School systems unavailable
- Significant safeguarding risk
- Operational disruption

Response:

- Immediate escalation
- Governors informed
- External agencies contacted

4. Immediate Response Steps

Upon discovery of a suspected cyber incident:

Step 1 – Report

Notify immediately:

- Business Manager
- Headteacher
- ICT Support Provider

Step 2 – Contain

Where advised:

- Disconnect affected devices from network
- Disable compromised accounts
- Prevent further access

Step 3 – Record

Record:

- Time identified
- Person reporting
- Systems affected
- Actions taken

Step 4 – Assess

Determine:

- Type of incident
- Systems affected
- Data involved
- Safeguarding implications

5. Escalation Contacts

Technical Support

ICT Support Provider

Safeguarding Concerns

Designated Safeguarding Lead

Current DSL:

Dawn Joy

Data Protection

School Data Protection Officer

Emergency Services

Police: 999

National Cyber Security Centre

Report serious cyber incidents where appropriate.

Information Commissioner's Office

Where personal data breach reporting thresholds are met.

6. Business Continuity Arrangements

If systems fail:

Attendance

- Manual class registers

Safeguarding

- Use existing paper safeguarding records if available
- Secure recording of new concerns

Communication

- School mobile phones
- Alternative email systems if available
- Parent communication through approved channels

Finance

- Delay non-essential transactions
- Manual purchasing process where required

7. Recovery

The ICT provider will:

- Remove malicious software
- Restore systems from backups
- Verify systems are secure
- Change compromised credentials
- Confirm network integrity

Before restoring services:

- ✓ Backups checked
- ✓ Security updates applied
- ✓ Password resets completed
- ✓ Incident investigation concluded

8. Post-Incident Review

Following any significant cyber incident:

The Business Manager will coordinate:

- Root cause review
- Lessons learned report
- Required policy updates
- Staff retraining where necessary

A summary report will be presented to governors.