I.T. Disaster Recovery Policy

KIBBLESWORTH ACADEMY

2026 2027

Author (s)	Craig Steel	
Updated by	Craig Steel	July 2026
Committee Approval		
Board Approval	Autumn Term 2026	
Chair of Trustees Signature		
Next Review Date:	Autumn Term 2027	
Review Cycle:	annual	

1. Purpose

This policy establishes the procedures for recovering the school's ICT infrastructure and digital services following a significant disruption, cyber incident, equipment failure or disaster.

The objectives of this policy are to:

- Protect critical educational and business operations.
- Minimise disruption to teaching and learning.
- Restore essential systems within agreed timescales.
- Protect the confidentiality, integrity and availability of data.
- Meet the expectations of the Department for Education (DfE) Cyber Security Standards regarding backup, recovery and business continuity planning. [gov.uk], [gov.uk], [cyber-secu...ion.gov.uk]

2. Scope

This policy applies to:

- School servers and network infrastructure
- Wireless networks
- Internet connectivity
- Microsoft 365 services
- Management Information Systems (MIS)
- Finance systems
- Safeguarding systems
- Telephony systems
- Backup systems
- School laptops, tablets and desktops

3. Definition of a Major ICT Incident

A major ICT incident is any event resulting in the loss, compromise or disruption of critical ICT services that significantly affects the school's ability to operate.

Examples include:

- Cyber attack or ransomware infection
- Loss of internet connectivity for an extended period
- Server failure

- Network outage
- Fire, flood or damage to ICT facilities
- Data centre outage
- Safeguarding system failure
- Major power disruption
- Loss of access to cloud services
- Large-scale hardware failure

4. Recovery Objectives

Recovery Time Objective (RTO)

The maximum acceptable period for restoring a service.

Service	Target RTO
Safeguarding systems	4 hours
Internet connectivity	4 hours
School email (Microsoft 365)	4 hours
MIS system	8 hours
Telephony	8 hours
Curriculum network	24 hours
Staff file storage	24 hours
Printing services	48 hours

These are target recovery times and may be affected by external factors.

Recovery Point Objective (RPO)

The maximum acceptable amount of data loss measured in time.

System	Target RPO
Safeguarding records	1 hour
MIS data	4 hours
Shared staff files	24 hours
Email services	24 hours
Curriculum data	24 hours

5. Disaster Recovery Team

Strategic Lead

Headteacher

Responsible for:

- Overall incident management
- Authorising major decisions
- Communications with governors
- Escalation to external agencies

Operational Lead

School Business Manager

Responsible for:

- Coordinating recovery activities
- Maintaining incident logs
- Liaison with ICT contractors
- Communicating service updates

Technical Lead

ICT Support Provider

Responsible for:

- Diagnosis of failures
- Technical recovery
- Restoration of services
- Cyber-security containment actions
- Backup restoration

Communications Lead

Administrative Officer

Responsible for:

- Staff updates
- Parent communications
- Website communications
- Telephone messaging updates

Safeguarding Lead

DSL

Responsible for:

- Assessing impact on safeguarding systems
- Implementing contingency safeguarding procedures
- Maintaining access to critical child protection information

---

6. Backup Strategy

The school will maintain backups in accordance with current DfE and NCSC recommendations.

The backup strategy will include:

- Daily automated backups
- Multiple backup copies
- Off-site backup storage
- Secure cloud backup services
- Regular backup testing
- Protection against ransomware attacks

The school will work towards the NCSC-recommended 3-2-1 backup model:

- Three copies of data
- Two different storage methods
- One copy stored off-site or in the cloud

This approach helps protect against cyber incidents, hardware failure, accidental deletion and local disasters. [cyber-secu...ion.gov.uk], [cyber-secu...ion.gov.uk]

7. Disaster Recovery Procedures

Phase 1 – Incident Identification

The person identifying the incident must:

1. Notify the Headteacher or SBM immediately.
2. Record:
    - Time discovered
    - Systems affected
    - Initial symptoms
    - Who reported it
3. Escalate to ICT support.

Phase 2 – Initial Assessment

The ICT Support Provider will determine:

- Nature of the incident
- Scope of impact
- Systems affected
- Risk to personal data
- Risk to safeguarding systems
- Whether external support is required

An initial severity level will be assigned:

Critical

Whole-school operations severely affected.

High

Significant service disruption.

Medium

Partial service loss.

Low

Limited operational impact.

Phase 3 – Containment

Where appropriate:

Cyber Incident

- Disconnect affected systems.
- Disable compromised accounts.
- Isolate infected devices.
- Preserve evidence and logs.

Network Failure

- Switch to alternative infrastructure if available.
- Reduce non-essential traffic.

Hardware Failure

- Remove failed equipment.
- Deploy replacement equipment.

Phase 4 – Recovery

Recovery shall follow the following order of priority:

Priority 1

Safeguarding and child protection systems.

Priority 2

Internet connectivity.

Priority 3

Email and communications systems.

Priority 4

MIS and attendance systems.

Priority 5

Finance systems.

Priority 6

Teaching and curriculum resources.

Priority 7

Non-essential services.

8. Ransomware Recovery Procedure

In the event of ransomware:

1. Disconnect affected devices immediately.
2. Do not pay any ransom demand.
3. Contact ICT support.
4. Notify the Headteacher and DPO.
5. Determine the source and spread of infection.
6. Restore systems from verified backups.
7. Conduct security review before reconnecting devices.
8. Consider reporting to relevant authorities where required.

9. Manual Continuity Arrangements

Where systems are unavailable:

Attendance

Paper registers will be used.

Safeguarding

DSLs will maintain temporary paper records.

Communication

Mobile phones and alternative email services may be utilised where appropriate.

Finance

Purchasing may be restricted until systems are restored.

10. Communications During a Major Incident

Stakeholder	Responsible Officer
Staff	Headteacher/SBM
Parents	Office Manager
Governors	Headteacher
DPO	Headteacher
ICT Support	SBM
Local Authority	Headteacher

Regular updates will be issued throughout recovery.

11. Testing and Validation

The disaster recovery process will be tested annually.

Testing may include:

- Backup restoration testing
- Simulated cyber incidents
- Server recovery exercises
- Business continuity scenarios

Results will be reported to governors.

Annual testing is consistent with DfE expectations for cyber resilience and backup recovery arrangements. [cyber-secu...ion.gov.uk], [cyber-secu...ion.gov.uk]

12. Post-Incident Review

Following any major ICT incident:

The Disaster Recovery Team will meet within 10 working days to:

- Review the response.
- Identify lessons learned.
- Assess recovery performance against RTO and RPO targets.
- Update policies and procedures.
- Produce a report for governors.

Appendix A – Emergency Contacts

Role	Name	Contact Number
Headteacher	Craig Steel	07425889388
SBM	Joanne Fairlamb	01914102975
ICT Support Provider	Omnicom	
DPO	Carole Connelly	01727572448
DSL	Craig Steel	07425889388
Chair of Governors	Emma Bulmer	01913887161
Local Authority Contact	Liz Simpson	Lizsimpson22@outlook.com