



Endeavour
Multi-Academy Trust



Cyber Security Policy

Endeavour Multi Academy Trust

DOCUMENT CONTROL		
Approved for operation within		Endeavour Multi Academy Trust
Version number		V1.0
Consulted on with recognised trade unions		N/A
Reviewed By		Trust Audit & Risk Committee
Recommended to Full Trust Board by:		N/A
Date approved by the Trust Board		N/A
Risk Register Item Number		N/A
Review Period		Annual
Next Review Date		Summer 2027
Policy status		Non-statutory
Location published		External
Owner		Trust Audit & Risk Committee
Author		Trust Estates Manager & Data Protection Officer
DOCUMENT HISTORY DATE	DOCUMENT VERSION	DOCUMENT HISTORY
04/05/2026	V1.0	New policy drafting to be used by all Endeavour MAT schools

1. Policy Statement

Endeavour Multi Academy Trust recognises its responsibility to protect the confidentiality, integrity and availability of digital information and systems. Cyber security is essential to safeguarding pupils, staff, operations, finances and reputation.

This policy sets out the framework for managing cyber risks across all academies within the Trust.

2. Scope

This policy applies to:

- All employees, trustees, governors, volunteers, contractors and third-party suppliers
- All pupils using Trust systems
- All Trust-owned or Trust-managed ICT systems, networks and data
- Personal devices used to access Trust systems is not encouraged.

3. Objectives

The objectives of this policy are to:

- Protect personal data in accordance with UK GDPR and the Data Protection Act 2018
- Reduce the risk of cyber security incidents, including ransomware and data breaches
- Ensure continuity of education and Trust operations
- Promote safe, responsible and secure use of technology

4. Governance and Responsibilities

4.1 Board of Trustees

- Holds ultimate accountability for cyber security and information risk
- Ensures appropriate policies, resources and assurance mechanisms are in place

4.2 Accounting Officer / CEO

- Overall responsibility for implementation of this policy
- Ensures cyber risks are included in the Trust risk register

4.3 Director of IT / Network Manager

- Implements technical security controls
- Monitors systems for vulnerabilities and incidents
- Oversees backup, patching and access control

4.4 Data Protection Officer (DPO)

- Advises on compliance with data protection legislation
- Assesses data breaches and liaises with the ICO where required

4.5 Heads of Academy

- Ensure policy compliance within their academy
- Promote cyber security awareness among staff and pupils

4.6 All Users

- Comply with this policy and related ICT policies
- Report suspected security incidents immediately

5. Legal and Regulatory Framework

This policy supports compliance with:

- UK GDPR
- Data Protection Act 2018
- Keeping Children Safe in Education (KCSIE)
- Prevent Duty
- National Cyber Security Centre (NCSC) guidance for schools
- ESFA Academy Trust Handbook

6. Risk Management

The Trust will:

- Identify and assess cyber risks regularly
- Maintain a risk register including cyber threats
- Apply proportionate technical and organisational controls
- Review risks annually or following significant change or incident

7. Access Control and Authentication

- Users will have **unique accounts**; shared accounts are prohibited
- Access will be **role-based** and granted on least-privilege principles
- Passwords must meet Trust-defined complexity standards
- Multi-Factor Authentication (MFA) will be used where technically feasible
- Accounts will be disabled promptly when users leave or change role

8. Device and Network Security

- Trust devices must be managed, encrypted and protected by anti-malware
- Security updates and patches must be applied promptly
- Firewalls, filtering and monitoring systems will be maintained
- Personal devices may only be used where formally approved and managed

9. Data Protection and Information Handling

- Personal and sensitive data must be stored securely
- Data must only be accessed for legitimate educational or operational purposes
- Sensitive data must not be transferred using unencrypted or unauthorised methods
- Cloud services must be approved and contracted in line with UK GDPR

10. Email and Phishing Protection

- Users must exercise caution with emails, attachments and links
- Phishing attempts must be reported immediately
- Suspicious emails must not be forwarded or responded to
- Regular awareness training will be provided

11. Remote Working and Home Learning

- Remote access must use secure authentication mechanisms
- Staff must ensure confidentiality when working off-site
- Devices used remotely must comply with Trust security standards

12. Backup and Business Continuity

- Critical systems and data will be backed up regularly
- Backups will be tested periodically
- Offline or immutable backups will be maintained
- Cyber recovery plans will align with the Trust Business Continuity Plan

13. Incident Management

All cyber security incidents, including suspected data breaches, must be reported immediately to:

- IT Support / Network Manager
- Data Protection Officer (where data is involved) (See GDPRiS below)

Incidents will be:

- Logged and investigated
- Contained and remediated

- Reported to external bodies (e.g. ICO, DfE) where legally required
- Reviewed to prevent recurrence
- All schools will use the GDPRiS platform for incident logging.

14. Training and Awareness

- Staff will receive cyber security awareness training at least annually (Staff are signposted to GDPRiS or National College training modules)
- Cyber security forms part of safeguarding and KCSIE compliance
- Pupils will be taught safe and responsible use of technology through the curriculum

15. Third-Party and Supplier Security

- Suppliers must demonstrate appropriate cyber security measures
- Data processing agreements will be in place where required
- Third-party access will be limited, monitored and reviewed
- RoPAs and DPIAs are stored for each school on the GDPRiS platform.
- DPIAs will be created before starting any new high-risk data processing activity

16. Compliance and Monitoring

- Compliance will be monitored through audits, reviews and assurance checks
- Breach of this policy may lead to disciplinary action
- Trustees will receive regular assurance on cyber security posture. DPO to re-report to the Trust board.

17. Policy Review

This policy will be:

- Reviewed annually by the Trust
- Updated following significant incidents, legal changes or technology changes

18. Related Policies

- Acceptable Use Policy (Staff and Pupils)
- Data Protection Policy
- Safeguarding and Child Protection Policy
- Business Continuity and Disaster Recovery Policy
- Remote Working Policy