

TITLE: Records Management Policy	REF:GOV004	VERSION:3
APPROVAL BODY: CEO	DATE: 24.02.26	REVIEW DATE: 23.02.27
LEAD PERSON: Data Protection Officer/Clerk		
VERSION	REVIEWER/APPROVAL	REVIEW NOTES
1. March 2018	Clerk/DPO/CEO	New Policy
2. March 2019	CEO	Review
3. February 2026	Clerk/DPO/CEO	Full review

RECORDS MANAGEMENT POLICY

Policy Statement

Activate Learning Education Trust recognises that effective records management is essential to:

- Compliance with legal and regulatory obligations
- Protection of personal data
- Good governance and accountability
- Educational and operational efficiency
- Protection of the rights of pupils, staff and stakeholders

The Trust is committed to managing its records in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018, and other applicable legislation.

Records are a corporate asset of the Trust and must be created, maintained, stored and disposed of in a secure and lawful manner.

Scope

This policy applies to:

- All academies within the Trust
- All Trustees, Members, Governors, employees, contractors and volunteers
- All records created, received or maintained in the course of Trust business

Records may be:

- Paper-based
- Electronic
- Audio/visual
- Email and digital communications
- Cloud-based records
- Safeguarding and SEN files

This policy applies regardless of format or storage location.

Definitions

Record

Any information created, received or maintained as evidence of the Trust's activities or legal

obligations.

Personal Data

Information relating to an identified or identifiable living individual.

Special Category Data

Personal data requiring additional protection, including health data, ethnicity, safeguarding information and SEN records.

Retention Schedule

The Trust's approved document specifying how long different categories of records must be kept and when they must be securely destroyed.

Legal and Regulatory Framework

This policy is designed to ensure compliance with:

- UK GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Limitation Act 1980
- Safeguarding and education legislation
- ICO guidance
- IRMS Toolkit for Schools

Where legislation conflicts, statutory obligations take precedence.

Data Protection Principles

All records containing personal data shall be managed in accordance with the following principles:

1. **Lawfulness, fairness and transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality**
7. **Accountability**

The Trust shall document lawful bases for processing in its Record of Processing Activities (ROPA).

Governance and Responsibilities

Board of Trustees

The Board retains ultimate accountability for records management compliance.

Chief Executive Officer

Ensures effective implementation across the Trust.

Data Protection Officer (DPO)

The DPO shall:

- Advise on compliance with UK GDPR
- Monitor adherence to this policy
- Provide guidance on retention and disposal
- Oversee data breach reporting
- Conduct audits where required

Headteachers / Senior Leaders

Responsible for:

- Local implementation
- Ensuring secure storage
- Compliance monitoring
- Staff awareness

All Staff

Must:

- Create accurate records
- Store records securely
- Follow retention schedules
- Report breaches immediately
- Dispose of records securely

Failure to comply may result in disciplinary action.

Records Creation and Maintenance

Records must:

- Be accurate and factual
- Be created only where necessary
- Not contain excessive personal data
- Be written professionally and objectively

Trust email accounts and systems must be used for official communications.

Retention and Disposal

The Trust shall maintain a Retention Schedule aligned with the IRMS Toolkit for Schools.

Retention

- Records shall not be kept longer than necessary.
- Retention periods shall be based on legal, regulatory and operational need.

Secure Disposal

When records reach the end of their retention period, they shall be:

- Shredded (paper records)
- Permanently deleted from systems
- Securely erased from devices
- Disposed of using approved confidential waste providers

A disposal log shall be maintained where appropriate.

Security of Records

The Trust shall implement appropriate technical and organisational measures to ensure security, including:

- Role-based access controls
- Strong password protocols
- Encryption where appropriate
- Locked cabinets for sensitive files
- Secure cloud storage
- Two-factor authentication (where applicable)
- Clear desk policy

Access to personal data shall be restricted on a need-to-know basis.

Special Category and Safeguarding Records

Special category and safeguarding records shall:

- Be stored separately where appropriate
- Have restricted access
- Be transferred securely
- Follow statutory retention requirements

Safeguarding files shall be transferred securely when a pupil moves school.

Data Subject Rights

Records management must support the Trust's obligations to uphold data subject rights, including:

- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure (where applicable)
- Right to restriction
- Right to object

Procedures for handling these rights are set out in the Trust's Data Protection Policy.

Data Breaches

Any loss, unauthorised disclosure or suspected compromise of records must be reported immediately to the DPO.

The Trust shall:

- Investigate all breaches
- Assess risk to individuals
- Notify the ICO within 72 hours where required
- Inform affected individuals where necessary

Records Sharing and Transfers

Where records are shared:

- A lawful basis must exist
- Data sharing agreements must be in place where required
- Transfers outside the UK must comply with UK GDPR transfer rules

Archiving

A percentage of records may be permanently preserved for historical purposes. Archiving shall:

- Be subject to appropriate safeguards
- Ensure personal data is anonymised where possible
- Comply with data protection legislation

Monitoring and Audit

The Trust shall:

- Conduct periodic audits
- Review retention compliance
- Monitor secure disposal
- Report compliance to Trustees

This policy shall be reviewed annually or sooner if required by legislative change.

Related Policies

- Data Protection Policy
- Freedom of Information Policy
- Data Breach Procedure
- IT Acceptable Use Policy
- Retention Schedule