Records Management Policy

Policy Owner:	Lighthouse Multi Academy Trust
Approved/ Ratified:	Pat Hunt
Review Dates:	July 2027

Document Version Control Log

Version	Modification Date	Synopsis of Changes
1.0	October 2025	
2.0	June 2026	Section 2- Legislation section added Section 3- added role of trustees, CEO, Trust Central Team and DPO Section 7- Updated section on removable media (USB and hard drives) Added Section 11- Associated Policies and Documents Strengthened sections throughout

Contents

1. Introduction and Scope

The Lighthouse Multi Academy Trust recognises records management as a core corporate function that supports the effective management of the Trust. A records management programme ensures that authoritative evidence of our work is created, captured, managed and made accessible within the scope of our information governance policy framework. This allows for improved accountability, transparency, continuity, decision-making, and better compliance with relevant legislation and regulations, as well as protecting the rights and interests of ourselves and our pupils.

A record is defined as information created, received and maintained as evidence and as an asset by the academy in pursuit of legal obligations or in the transaction of business. Records are retained as evidence for a set period determined by legal, regulatory and functional requirements.

The Records Management policy and retention schedule applies to all records created, received or maintained by the Trust in the course of carrying out its functions, regardless of whether it is in paper or electronic format.

This policy applies to all employees, governors or Trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the academy. It should be read alongside the other policies within our information governance policy framework, including the Data Protection policy, Information Security policy and Online Safety and acceptable use policy.

2. Legislation and Guidance

This policy has regard to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Limitation Act 1980
- Education (Pupil Information) (England) Regulations 2005
- Keeping Children Safe in Education
- Working Together to Safeguard Children
- Information Commissioner's Office (ICO) guidance
- Department for Education Record Keeping and Management Guidance
- Academy Trust Handbook

3. Roles and Responsibilities

Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant legislation relating to records management, information governance and data protection. The Board is responsible for:

- approving the Trust's Records Management Policy and reviewing it at appropriate intervals;
- ensuring that effective governance arrangements are in place for the management of records across the Trust;
- receiving assurance that records are managed securely, retained appropriately and disposed of in accordance with legal and regulatory requirements; and
- ensuring sufficient resources are available to support effective records management across the Trust.

Chief Executive Officer (CEO)

The Chief Executive Officer has overall executive responsibility for ensuring that this policy is implemented consistently across the Trust and that appropriate arrangements are in place to support compliance.

Trust Central Team

The Trust Central Team supports the implementation of this policy by:

- developing and maintaining Trust-wide records management procedures;
- providing advice, guidance and support to academies;
- maintaining Trust-wide records management documentation where appropriate;

- monitoring compliance and coordinating policy reviews; and
- supporting academies with records retention, secure disposal and information governance matters.

Senior Information Risk Owner (SIRO)
The SIRO is responsible for overseeing the implementation of this policy and ensuring that effective records management practices are in place across the Trust. They are ultimately responsible for the day-to-day operational management of the Trust and will ensure that staff are appropriately trained in relation to records management, supported by the SPOC and IAOs. In the Lighthouse Multi Academy Trust this role lies with the CEO or appropriate member of the Trust Central Team.

Single Point of Contact (SPOC)
The SPOC will support the SIRO in the day-to-day operational management of the academy, providing guidance on good records management practices and promoting compliance with this policy so that information can be retrieved easily, appropriately and in a timely way. They will help develop and carry out regular reviews of the records management programme, at least annually, to ensure compliance and to check that records are stored securely and can be accessed appropriately. In each academy this role lies with the Executive Headteacher/ Headteacher or appropriate delegate (DHT, AHT, SBM).

Information Asset Owner (IAO)
The IAO is responsible for the security and maintenance of a particular record during its lifecycle. They need to understand how information is created, amended or added to over time, and know who has access to the records and why. They are responsible for the appropriate disposal of information when it is no longer required. In each academy this role lies with the Executive Headteacher/ Headteacher.

Data Protection Officer (DPO)
The Data Protection Officer provides independent advice on data protection legislation and supports compliance where records contain personal data. The DPO monitors compliance with UK GDPR and the Data Protection Act 2018 and advises on records management where personal information is involved.

All staff
All staff, including governors or Trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the academy are responsible for managing records consistently in accordance with this policy. They must keep complete and accurate records which adequately document their work.

All staff must:
- create and maintain accurate records that adequately document their work;
- store records securely;
- follow the Trust's Records Retention Schedule;
- dispose of records securely when authorised;
- protect confidential and personal information; and
- report any records management or information security concerns promptly.

4. Records Management
We have a robust programme in place for managing our records throughout their lifecycle. This includes using methods such as version control and file plans to ensure that records can be easily searched and accessed in the event of an information request. Information governance risks are recorded and reviewed through the Trust's risk management processes.

Records include emails, cloud storage, Microsoft 365 documents, SharePoint, Teams conversations where they form part of the official business record, management information systems, CCTV, safeguarding systems and approved digital platforms.

Good records management supports compliance with Subject Access Requests, Freedom of Information requests, complaints, audits and inspections.

Information Asset Register (IAR)

The Trust maintains an Information Asset Register (IAR) to identify and manage its information assets and records. The register supports effective records management by documenting the information held by the Trust, where it is stored, the responsible information asset owner, security arrangements, and the applicable retention and disposal requirements.

Where personal data is processed, the Information Asset Register also forms part of the Trust's **Record of Processing Activities (ROPA)** in accordance with Article 30 of the UK General Data Protection Regulation (UK GDPR).

The Information Asset Register is reviewed at least annually, and whenever significant changes occur to systems, services, business processes or legislation, to ensure it remains accurate and supports the Trust's records management, information governance and statutory compliance obligations.

Email management

We have a process in place to ensure that emails are also managed in line with this policy and our retention schedule. Emails discussing academy business or reflecting significant actions or decisions concerning academy business will not be stored in personal email inboxes but will be removed and stored securely in the appropriate filing system.

Personal Academy email inboxes are regularly reviewed by staff to ensure any unnecessary emails are deleted.

Where Microsoft Teams conversations contain official decisions or business records these should be retained within the appropriate Trust system where required.

5. Pupil Records

Academies are under a duty to maintain a record for each pupil which serves as the core record of an individual’s progress through the education system and should accompany them throughout their academy career. The information within the pupil record must be easy to find, accurately and objectively recorded, and expressed in a professional manner.

Pupil records are held electronically within our management information system (MIS). Some information, not forming part of the core record, will be held outside the MIS in either electronic or paper format. This includes information which has shorter retention periods such as attendance registers, consent forms, medical forms, accident forms, absence notes and pupil work.

Safeguarding files

Records relating to pupils involved with child protection or safeguarding are held securely in a designated system (CPOMs) accessible to the Designated Safeguarding Leads (DSLs). This is stored separately to the core pupil record to ensure confidentiality and restricted accessibility.

6. Staff Records

Records relating to the academy workforce will be held securely, either electronically or in paper format, with appropriate measures in place to ensure accessibility is restricted.

7. Storage and Security

All records, especially where containing personal data, will be stored securely to maintain confidentiality, whilst also keeping information accessible to those authorised to see it. Electronic records will have appropriate security and access controls in place, and systems will have robust audit functions in place wherever possible.

Paper records will be stored in secure, lockable storage areas with restricted access.

Electronic records will be subject to appropriate backup, disaster recovery and cyber security arrangements to ensure records remain accessible where required.

When sharing or transferring records containing personal information, we will ensure appropriate transmission security controls are in place, in line with our Information Security Policy.

The Trust will follow the DfE Cyber Security Standards for Schools and Colleges to ensure records remain secure against unauthorised access, ransomware and other cyber threats.

Records created or amended using approved AI systems remain official Trust records. Staff remain responsible for ensuring their accuracy before storage.

Access to electronic records will be controlled through role-based permissions, strong authentication and encryption where appropriate.

Use of Removable Media

Removable storage devices, such as Trust-approved encrypted USB sticks and external hard drives, must only be used for temporary storage where there is a legitimate need.

Staff must transfer all Academy records and information held on removable media to the designated Academy storage system as soon as practicable and within the timescales set out by the Academy. Removable media must not be used as a permanent storage location for Academy records.

The Academy will maintain a register of approved removable storage devices, including device identifiers and serial numbers, and will record the issue and return of each device.

A review period will be applied to all issued removable media to ensure that any information required for ongoing educational purposes has been transferred to the appropriate storage location. Once information has been transferred and is no longer required on the device, the removable media will be securely wiped in accordance with the Academy's information security and records disposal procedures before being returned or reissued.

8. Retention and Disposal

Retention is the period a record is kept for after it stops being actively used, but before it is destroyed. Retention is a vital part of records management as it allows organisations to retain records only for as long as needed, and discourages records being kept for long periods 'just in case'.

The retention period for particular types of records is determined by legal, regulatory or functional requirements. We have implemented a Retention Schedule which sets out our specified retention periods (Appendix A). Where records are subject to litigation, complaints, safeguarding investigations, disciplinary proceedings, ICO investigations or police enquiries, disposal will be suspended until the matter has concluded.

We will ensure that any records containing personal or confidential information are disposed of appropriately and securely when they have reached the end of their retention period, in line with our retention schedule.

Records held in databases or electronic management systems with the functionality for automatic destruction of records after a specified period of time will be used wherever possible. A review of the records will be carried out prior to destruction, where practical.

Where automatic disposal is not in place, for example for paper records, we will carry out a manual review, at least annually, to ensure they are deleted in line with retention guidelines.

The disposal of all information is documented to ensure that we maintain a record of when it has been deleted and by whom. This allows us to evidence that a record no longer exists, or has been transferred to another institution, in the event of a subject access or Freedom of Information request being received.

9. Archiving

A small percentage of our records will be selected for preservation as part of The Lighthouse Multi Academy Trust's wish to create and preserve an organisational memory of its history, including its pupils and staff. This organisational memory is expected to contribute to the wider social memory of the community which the academy serves.

Records containing personal information will only be selected for archive with appropriate safeguards in place to protect the rights and freedoms of individuals. This will include anonymisation or pseudonymisation wherever possible

Historical records may be retained permanently where they have enduring historical, legal or research value.

10. Training

Since all employees are involved in creating, maintaining and using records, it is vital that everyone understands their record management responsibilities as set out in this policy. We will ensure that staff are appropriately trained or experienced and that they understand the need for effective record keeping.

When we introduce new technology or ICT systems we ensure that users are appropriately trained to use these systems and can manage records within them effectively.

Assurance
The Lighthouse Multi Academy Trust will conduct termly assurance exercises and provide evidence to Trustees of these checks.

Pupil records: Compliance audits of pupil electronic records (through Arbor) will be checked termly by the Trust Central Team to ensure we hold all statutory information:

- At least 2 contact numbers for each pupil
- All fields are completed

Staff Records: Spot checks on people compliance reviews will be conducted every 6 months by the Director of People and Culture and reported to Trustees. This will cover:

- DBS checks
- Right to work
- Self declarations
- ID
- References
- Overseas checks
- Online searches

The Director of Safeguarding and Attendance will also check this through the Single Central Record checks (SCR).

Safeguarding Files: The Director of Safeguarding and Attendance regularly seeks assurances of all children's safeguarding files. A termly visit will be undertaken where safeguarding files will be checked to ensure that it meets the DFE information sharing guidance.

- Open and transparent
- Seek advice when unsure
- Share with consent where possible
- Balance safety and privacy
- Sharing information when needed
- Timely and secure
- Document the sharing process and rationale

11. Associated Policies and Documents

This policy should be read in conjunction with the following policies, procedures, and guidance:

- Trust Data Protection Policy
- Trust Information Security Policy
- Trust Acceptable Use Policy (AUP)
- Trust Freedom of Information Policy
- Trust Privacy Notices
- Trust Cyber Security Policy
- Trust Social Media Policy
- Trust Mobile Phone Policy
- Trust Admissions Policy
- Academy GDPR Policy
- Academy CCTV Policy
- Academy Safeguarding and Child Protection Policy
- Academy Business Continuity and Disaster Recovery Plan
- Trust Staff Code of Conduct

The Academy may also have regard to guidance issued by the Information Commissioner's Office (ICO), the Department for Education (DfE), and other relevant regulatory bodies.

Appendix A– Retention Schedule (statutory retention periods)

The following records have statutory retention periods.

This list has been taken from the DfE’s Record Keeping and Management guidance: https://www.gov.uk/guidance/data- protection-in-schools/record-keeping-and-management (updated June 2025)

Where there is any conflict between statutory retention requirements and this schedule, statutory requirements take precedence.

Pupil records

Document type	Retention period	Action at end of retention period	Further information
Primary school pupil records	Until the pupil leaves the academy.	Transfer to secondary school or other primary school when the pupil leaves.	See The Education (Pupil Information) (England) Regulations 2005 for details of what to keep in the pupil record. There is guidance on how to transfer information to another academy.
Secondary school pupil records	Until the pupil’s 25th birthday.	Dispose of records securely. If the pupil leaves to go to another academy, transfer the records to that school. There is guidance on what to do if the school closes before the end of the retention period.	See The Education (Pupil Information) (England) Regulations 2005 for details of what to keep in the education record. Retain as detailed in section 2 of the Limitation Act 1980.

Document type	Retention period	Action at end of retention period	Further information
Special educational needs and disabilities (SEND), including SEND statements and accessibility plans	Until the pupil's 30th birthday.	Dispose of records securely, unless the document is subject to a legal hold. If the pupil leaves to go to another academy, transfer the records to that academy.	SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980.
Attendance and absence	Until the pupil's 30th birthday.	Dispose of records securely, unless the document is subject to a legal hold. If the pupil leaves to go to another academy, transfer the records to that academy.	SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980.

Child protection records

Document type	Retention period	Action at end of retention period	Further information
Child protection files	Until the child's 25th birthday. If the file relates to child sexual abuse, retain until the child's 75th birthday.	Dispose of records securely. Child protection files should be passed on to any new academy a child attends. This should be transferred separately from the main pupil file.	Should be stored in a separate child protection file. Keeping children safe in education sections 66, 67, 121 and 122. The Report of the Independent Inquiry into Child Sexual Abuse (IICSA), recommendation on access to records.
Allegations of child protection against a member of staff, including unfounded allegations	Until the staff member's normal retirement age, or 10 years from the date of the allegation, whichever is later.	Dispose of records securely.	Keeping children safe in education. Working together to safeguard children.

Finance records

Document type	Retention period	Action at end of retention period	Further information
Contracts	6 years from the last payment on the contract.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Debtor's records	6 years from the end of the financial year.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
VAT records	6 years from the end of the financial year.	Dispose of records securely.	May include invoices, budgets, bank statements and annual accounts. Record keeping (VAT Notice 700/21).

Governance records

Document type	Retention period	Action at end of retention period	Further information
Admissions	3 years from the admission date.	Dispose of records securely.	Working together to improve school attendance.
Attendance registers	3 years from the date of entry.	Dispose of records securely.	Regulation 14 of the Education (Pupil Registration) (England) Regulations 2006.
Annual governors report	10 years.	Dispose of records securely.	The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002. Retain as detailed in section 2 of the Limitation Act 1980.
Curricular record	At least one year.	Dispose of records securely.	The Education (School Records) Regulations 1989. Regulation 3 of the Education (Pupil Information) (England) Regulations 2005.
Directors – disqualification	15 years from the date of disqualification.	Dispose of records securely.	The Education (Company Directors Disqualification Act 1986: Amendments to Disqualification Provisions) (England) Regulations 2004

Document type	Retention period	Action at end of retention period	Further information
Records of educational visits	10 years from the date of the visit. If there was an incident on the visit, retai the permission slips for al pupils and the incident report in the pupil record, or until the pupil reaches the age of 25.	Dispose of records securely.	Health and safety on educational visits. Retain as detailed in section 2 of the Limitation Act 1980.
School vehicles	6 years from the disposal of the vehicle.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Statutory registers and compliance	Retention periods vary, for example: Memorandums of understanding should be retained for the life of the academy plus 6 years. Annual reports should be retained for 10 years from the date of the report. Board meeting records should be retained for 10 years from the date of the meeting.	Dispose of records securely.	May include annual reports and governance records. Companies Act 2006 contains information on which statutory registers to keep. Compliance guidance in the maintained schools governance guide. Compliance guidance in the academy trust governance guide. Academy trust handbook.

Health and safety records

Document type	Retention period	Action at end of retention period	Further information
Accessibility plans	Life of plan plus 6 years.	Dispose of records securely.	Retain as detailed in section 2 of the Limitation Act 1980.
Accident records	3 years from the date of the accident.	Dispose of records securely.	Accidents involving pupils should be retained in the pupil record. Regulation 25 of the Social Security (Claims and Payments) Regulations 1979.
Monitoring exposure to substances hazardous to health, including asbestos	5 years.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002.
Health surveillance records	40 years.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002. Health surveillance - Record keeping.
Other health records of staff	While the worker is employed in your academy.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002. Health surveillance - Record keeping.

Document type	Retention period	Action at end of retention period	Further information
Fire assessments	Life of the risk assessment plus 6 years.	Dispose of records securely.	Fire Service Order 2005. Retain as detailed in section 2 of the Limitation Act 1980.

Property records

Document type	Retention period	Action at end of retention period	Further information
Maintenance records	6 years from the end of the financial year.	Dispose of records securely.	Record keeping (VAT Notice 700/21).
Title deeds	12 years from the end of the deed.	Dispose of records securely.	Section 2 of the Limitation Act 1980.

Staff records

Document type	Retention period	Action at end of retention period	Further information
Copies of DBS certificates	6 months from the date of recruitment.	Dispose of records securely.	Keeping children safe in education.
Maternity pay records	3 years after the end of the tax year in which the maternity pay period ends.	Dispose of records securely.	The Statutory Maternity Pay (General) Regulations 1986.
Pay records	3 years from the end of the tax year they relate to.	Dispose of records securely.	PAYE and payroll for employers: Keeping records.
Personnel files	6 years from termination of employment.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Retirement benefits	A minimum of 6 years from the end of the year in which the accounts were signed.	Dispose of records securely.	Regulation 15 of the Retirement Benefits Schemes (Information Powers) Regulations 1995.

Please contact the Head of Governance or the Operations and Compliance Manager for advice regarding non- statutory retentions periods.