Four Hills Education Trust
Where Every Step is Shaped with CARE

Records Management and Information Retention Policy

Policy reference: RM-24 | Version 4.0

Effective from 1 September 2026

Document control	Details
Policy owner	Chief Finance and Operations Officer
Operational lead	Data Protection Officer and Chief Finance and Operations Officer
Approval body	Audit and Risk Committee / Board of Trustees
Approval date	To be completed on approval
Review cycle	Annual, or earlier following legal, regulatory or operational change
Next review	September 2027
Applies to	The Trust, all academies, central services, Members, Trustees, Governors, employees, volunteers, contractors and processors
Related documents	Data Protection Policy; Information Security Policy; Freedom of Information Policy; Financial Regulations; Scheme of Delegation; Business Continuity Plan; Safeguarding and HR policies

Status

This policy replaces Records Management Policy V3. It must be read with Appendix 1, the Trust Information Retention Schedule. Where legislation, an active investigation or a formal preservation hold requires longer retention, that requirement takes precedence.

Contents

1. Purpose and objectives

Four Hills Education Trust recognises records as corporate assets and evidence of its educational, safeguarding, employment, governance and financial activities. Effective records management enables the Trust to operate efficiently, protect individuals, demonstrate accountability and provide reliable evidence to trustees, regulators, auditors and other authorised bodies.

- ensure records are authentic, accurate, complete, accessible and secure throughout their lifecycle;
- retain records for no longer than necessary, unless a legal, contractual, safeguarding, audit or public-interest requirement applies;
- support compliance with data protection, freedom of information, company, charity, education, safeguarding, employment, tax and financial reporting requirements;
- support regularity, propriety, value for money, effective internal control and auditability;
- ensure secure, consistent and documented disposal; and
- preserve records of enduring legal, governance or historical value.

2. Scope

This policy applies to all records created, received or maintained by or on behalf of the Trust, regardless of format, location or ownership of the device or system used. It covers paper and electronic records, email, instant messages, Teams chats, SharePoint, OneDrive, finance and payroll systems, management information systems, safeguarding systems, CCTV, audio and video, photographs, databases, portable media and records held by third-party processors.

It applies to Members, Trustees, local governors, employees, agency workers, volunteers, consultants, contractors and any other person processing records on behalf of the Trust. Personal

notes become Trust records where they evidence decisions, actions, advice, incidents or official business.

3. Legal and regulatory framework

The Trust will manage records in accordance with applicable requirements, including:

- UK General Data Protection Regulation and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025;
- Freedom of Information Act 2000 and Environmental Information Regulations 2004;
- Companies Act 2006 and applicable company-record requirements;
- Charities Act 2011 and charity accounting and governance requirements;
- Education legislation, funding agreements and Department for Education requirements;
- Academy Trust Handbook, including the version effective at the relevant time;
- Academies Accounts Direction, model accounts and external audit requirements;
- HM Revenue and Customs requirements, pension requirements and employment law;
- Keeping Children Safe in Education and other safeguarding requirements;
- Limitation Act 1980 and other applicable limitation periods; and
- contractual, grant, insurance and regulatory conditions applying to particular records.

The Academy Trust Handbook 2025 applies from 1 September 2025. The Academy Trust Handbook 2026 takes effect on 1 October 2026. The Trust will apply the current version and implement new requirements by their effective date.

4. Records management principles

Principle	Trust requirement
Lawfulness, fairness and transparency	Records containing personal data must be created and used for lawful, clear and documented purposes.
Purpose limitation	Records must not be reused incompatibly without a lawful basis and appropriate transparency.
Data minimisation	Only information necessary for the business purpose should be recorded.
Accuracy	Records must be factual, clear, attributable, dated and corrected where inaccurate without obscuring the audit trail.
Storage limitation	Retention must be justified, documented and reviewed. Personal data must be erased or anonymised when no longer required.
Integrity and confidentiality	Records must be protected against unauthorised access, alteration, loss, destruction or disclosure.
Accountability	The Trust must be able to demonstrate decisions, controls, retention and disposal.
Authenticity and auditability	Records must reliably evidence who created or changed them, when and why.

5. Governance, roles and responsibilities

Role	Responsibilities
Board of Trustees	Approve the policy; ensure resources and oversight; hold the Accounting Officer to account; receive assurance through the Audit and Risk Committee.
Audit and Risk Committee	Oversee records risks relevant to internal control, financial assurance, audit evidence and regulatory compliance; monitor significant findings and actions.
Accounting Officer / CEO	Ensure Trust-wide implementation, accountability and escalation of serious non-compliance.
Chief Finance and Operations Officer	Policy owner; ensures financial, procurement, payroll, asset and governance records support audit and regulatory obligations; maintains disposal governance with the DPO.
Data Protection Officer	Advises on data protection, retention, information rights and breaches; monitors compliance independently; supports audits and preservation decisions.
Headteachers and central directors	Act as Information Asset Owners for their services unless assigned otherwise; ensure local implementation, access control, review and disposal.
Governance Professional	Maintains definitive governance records, registers, minutes, attendance and publication evidence.
School Business Managers / Records Coordinators	Coordinate local inventories, retention reviews, disposal logs, transfers and staff guidance.
All users	Create accurate records; use approved systems; follow retention, security and disposal requirements; report incidents promptly.
Processors and contractors	Comply with written instructions and contracts; protect, return or securely delete records; provide evidence of deletion when required.

6. Information asset management

The Trust will maintain a proportionate Information Asset Register and Records of Processing Activities identifying key record sets, owners, systems, purposes, lawful bases, sensitivity, recipients, retention rules, locations, processors and international transfers. Asset owners must review entries at least annually and when systems or processing change.

New systems, projects or significant changes must consider retention, deletion, export, audit trails, business continuity and information rights from the design stage. A Data Protection Impact Assessment must be completed where processing is likely to result in high risk to individuals.

7. Records lifecycle

7.1 Creation and capture

- Create records promptly and in an objective, professional and intelligible manner.
- Record significant decisions, approvals, advice, challenge, financial authorisation and the reasons for them.
- Use approved templates, classifications, metadata and version controls.
- Capture substantive email, chat or informal-channel decisions into the authoritative corporate record.
- Avoid unnecessary duplication and do not retain convenience copies beyond operational need.

7.2 Classification, filing and retrieval

Records must be stored in approved Trust systems and organised so they can be located promptly for operational, safeguarding, audit, Subject Access, Freedom of Information, litigation and regulatory purposes. Official records must not be held solely in personal mailboxes, local device drives or unapproved consumer storage.

7.3 Maintenance and quality

- Access permissions must be role-based and reviewed regularly.
- Changes must preserve an appropriate audit trail.
- Superseded drafts should be removed when no longer needed, while final approved versions are retained.
- Record movements and off-site storage must be traceable.
- Owners must periodically review accuracy, sensitivity, accessibility and continuing need.

7.4 Closure and archiving

Record sets must have a defined closure trigger, such as pupil leaving date, employment end date, contract expiry, completion of a project, financial year end or closure of a case. Closed records must be protected from inappropriate alteration and archived where continued retention is required.

8. Access, disclosure and information rights

Access is permitted only where required for authorised duties. Disclosure must have a documented lawful basis, be necessary and proportionate, and use a secure transfer method. A record of significant external disclosures must be maintained where appropriate.

Subject Access Requests, data protection rights requests, Freedom of Information requests, Environmental Information requests, legal disclosure requests and regulatory notices must be referred immediately to the DPO and relevant senior lead. No records potentially within scope may be altered or deleted after a request is received or reasonably anticipated.

9. Security, storage and business continuity

- Use Trust-approved systems, encryption and secure transfer methods appropriate to the risk.
- Apply least-privilege access, multi-factor authentication where available, and prompt removal of access when roles end or change.
- Protect paper records in secure storage with controlled keys or access.
- Maintain backups, recovery procedures and tested business continuity arrangements.

- Do not use personal email, personal cloud storage or unauthorised removable media for Trust records.
- Ensure third-party contracts address confidentiality, security, retention, deletion, breach reporting, audit and return of records.
- Report lost, misdirected, corrupted or inappropriately accessed records immediately under the data breach procedure.

10. Retention, review and disposal

Appendix 1 sets the Trust's standard minimum retention periods. A longer period may apply where required by law, contract, funding condition, safeguarding need, insurer, auditor, regulator, active complaint or preservation hold. Records must not be retained indefinitely merely because they may be useful.

10.1 Review

Information Asset Owners must ensure scheduled reviews take place at least annually. Review may result in secure destruction, anonymisation, extension with recorded justification, transfer to another controller, or permanent preservation.

10.2 Secure disposal

- Paper containing confidential information must be cross-cut shredded or disposed of through an approved confidential-waste provider.
- Electronic records must be securely deleted from live systems and, where technically feasible and proportionate, from scheduled backups in line with backup cycles.
- Physical media and equipment must be sanitised or destroyed through approved arrangements.
- Disposal of significant record sets must be authorised and entered in the disposal log.
- Processors must provide deletion or return assurance where required by contract.

11. Preservation holds and exceptions

Routine disposal must stop immediately for records relevant to actual or reasonably anticipated litigation, safeguarding investigations, complaints, employment proceedings, whistleblowing, fraud, audit, insurance claims, police or regulatory enquiries, Subject Access Requests, Freedom of Information requests or other formal investigations.

The DPO, CFOO, CEO, legal adviser or other authorised senior officer may issue a written preservation hold. The hold must identify scope, owners, systems and review date. Disposal may recommence only when the hold is formally released. Records retained beyond the normal period must have the reason, authority and review date documented.

12. Financial, governance and academy trust records

The Trust must maintain adequate accounting records and evidence supporting transactions, balances, approvals, regularity, propriety and value for money. Records must be sufficient for management oversight, internal scrutiny, external audit, DfE/ESFA review and preparation of annual accounts and returns.

- Maintain a clear audit trail from source documentation through authorisation, accounting entry, reconciliation and reporting.

- Retain procurement, tender, quotation, contract, related-party, payroll, grant, income, banking, asset and journal evidence in accordance with Appendix 1 and any longer contractual or grant condition.
- Keep signed annual accounts, governing documents, definitive board and committee minutes, statutory registers and other enduring corporate records permanently.
- Provide records requested by DfE, ESFA, auditors or other authorised bodies promptly and in an accessible form.
- Ensure records supporting annual accounts comply with the Academies Accounts Direction and current Academy Trust Handbook.

13. Monitoring, assurance and training

- Mandatory induction and periodic refresher training for staff with records responsibilities.
- Annual Information Asset Register and retention review.
- Risk-based sample checks of record quality, access, retrieval, retention and disposal.
- Periodic testing of backup restoration and business continuity.
- Reporting of significant weaknesses, overdue actions and serious breaches to the Audit and Risk Committee.
- Review of processor compliance and deletion evidence.

14. Breaches and non-compliance

Failure to follow this policy may expose the Trust and individuals to legal, safeguarding, financial, audit and reputational risk. Suspected non-compliance must be reported promptly. Deliberate or negligent breaches may be addressed under disciplinary, contractual or governance procedures. Personal data breaches will be assessed and, where required, reported to the Information Commissioner's Office and affected individuals within applicable legal timescales.

15. Policy review

This policy will be reviewed annually and sooner where legislation, DfE requirements, the Academy Trust Handbook, the Academies Accounts Direction, technology, organisational structure or risk changes. The current approved version must be made available to relevant staff and governance bodies.

Appendix 1: Information Retention Schedule

The periods below are standard minimums and should be applied from the stated trigger. “Current year + 6 years” means the record is retained for the remainder of the current financial year and six complete financial years after it. Where another legal or contractual period is longer, or a preservation hold applies, retain for the longer period. Before disposal, confirm that no audit, claim, investigation, safeguarding matter or information request is open or reasonably anticipated.

Category	Record	Minimum retention	Trigger / notes
Corporate and governance	Articles of association, funding agreements, deeds, trust establishment and title documents	Permanent	Creation / execution Original corporate evidence; secure archival copy.
Corporate and governance	Signed board, committee and members’ minutes; written resolutions	Permanent	Meeting / resolution date Retain definitive signed or approved version.
Corporate and governance	Board and committee papers supporting decisions	Permanent where material; otherwise 6 years	Meeting date Preserve papers needed to understand significant decisions.
Corporate and governance	Statutory registers, trustee/member appointment and resignation records	Permanent	Creation / cessation Subject to lawful access and publication requirements.
Corporate and governance	Declarations of interests and related-party declarations	Current year + 6 years	Superseded / end of service Longer where linked to a transaction or investigation.
Corporate and governance	Governance attendance, skills audits and training records	6 years	End of academic year / service Retain sufficient audit evidence.
Finance and audit	Signed annual report and financial statements	Permanent	Financial year end Corporate and historical record.
Finance and audit	General ledger, trial balance, journals, reconciliations and working papers	Current year + 6 years	Financial year end Longer if tax, grant, asset or legal requirements apply.
Finance and audit	Purchase invoices, sales invoices, receipts, credit notes and payment evidence	Current year + 6 years	Financial year end Maintain complete audit trail.
Finance and audit	Bank statements, mandates, BACS reports and cash records	Current year + 6 years	Financial year end Protect banking credentials and access data.

Category	Record	Minimum retention	Trigger / notes
Finance and audit	Budget, forecasts, management accounts and monitoring reports	Current year + 6 years	Financial year end Permanent where integral to major strategic decisions.
Finance and audit	Internal scrutiny, external audit files, management letters and action evidence	Current year + 6 years	Completion / financial year end Signed final reports may be permanent where significant.
Finance and audit	Grant claims, allocations and supporting evidence	Current year + 6 years minimum	Grant end / financial year end Apply longer period stated by grant funder.
Finance and audit	VAT, tax and HMRC records	At least 6 years	End of relevant accounting period Apply specific HMRC requirements where longer.
Payroll and pensions	Payroll records, gross-to-net reports, deductions, RTI and payment evidence	Current year + 6 years	Financial year end Pension or tax requirements may require longer.
Payroll and pensions	Pension records supporting membership, contributions and service	Scheme requirement; normally employment + 6 years minimum	Employment end / final payment Check Teachers' Pensions or LGPS requirements.
Procurement and contracts	Tender, quotations, evaluation, approvals, due diligence and award records	Contract end + 6 years	Contract expiry / termination 12 years where executed as a deed; longer for major works or claims.
Procurement and contracts	Contracts and variations executed under hand	Contract end + 6 years	Expiry / termination Retain with procurement and performance evidence.
Procurement and contracts	Contracts and deeds executed as deeds	Contract end + 12 years	Expiry / termination Subject to legal advice and limitation rules.
Procurement and contracts	Supplier performance, disputes and contract-management records	Contract end + 6 years	Expiry / resolution Longer if dispute or claim remains possible.
Assets and estates	Fixed asset register	Life of asset + 6 years	Disposal / derecognition Retain acquisition, valuation, funding and disposal evidence.

Category	Record	Minimum retention	Trigger / notes
Assets and estates	Property deeds, leases, title, planning and major building records	Permanent or property interest + 12 years	Disposal / lease end Seek legal advice before disposal.
Assets and estates	Routine maintenance and minor works records	6 years	Completion Longer for warranties, claims or statutory inspection.
Assets and estates	Asbestos, fire, legionella, electrical, gas and statutory compliance records	As required by specific law; otherwise life of premises/system + 6 years	Superseded / disposal Do not dispose without estates and H&S review.
HR and workforce	Recruitment records for unsuccessful applicants	6 months after appointment	Recruitment decision Extend to 12 months only with documented justification.
HR and workforce	Personnel file and employment contract records	Employment end + 6 years	Employment end Safeguarding or pension records may require longer.
HR and workforce	Right-to-work check evidence	Employment end + 2 years	Employment end Apply current Home Office requirement.
HR and workforce	DBS certificate copy	Normally no longer than 6 months	Recruitment / check decision Retain check outcome and required SCR evidence, not certificate, unless exceptional lawful reason.
HR and workforce	Single Central Record	Current record plus historic audit evidence for 6 years	Superseded / employment end Protect access; preserve evidence of checks.
HR and workforce	Disciplinary, grievance and capability records	Employment end + 6 years	Case closure / employment end Remove spent warnings from active use as policy requires, while preserving restricted legal record if justified.
HR and workforce	Sickness absence and occupational health records	Employment end + 6 years	Employment end Longer where health surveillance law applies.
HR and workforce	Accident records involving staff	At least 3 years; 6 years preferred for claim defence	Incident date Longer for minors, reportable incidents or active claims.

Category	Record	Minimum retention	Trigger / notes
Pupils and education	Main pupil educational record	Transfer to next school; receiving setting retains under its schedule	Pupil leaves Transfer securely and record the transfer.
Pupils and education	Attendance registers	6 years from date of entry	Date of entry / academic year end Apply current statutory attendance requirements.
Pupils and education	Admissions records for admitted pupils	Pupil leaves + 6 years	Pupil leaves Key information may form part of pupil record.
Pupils and education	Admissions records for unsuccessful applicants	Appeal period + 1 year, normally no more than 2 years	Decision / appeal closure Retain longer only for live challenge or legal reason.
Pupils and education	Assessment and curriculum records not transferred	Pupil leaves + 6 years or as required by DfE	Pupil leaves Avoid duplicate retention where transferred into main record.
SEND	EHCP and significant SEND records	Transfer with pupil; copy only where legally required, then pupil age 25 recommended	Pupil leaves / age 25 Apply local authority and safeguarding advice.
Safeguarding	Child protection and safeguarding file	Transfer securely to next setting; receiving setting retains until 25th birthday or longer if required	Pupil leaves / 25th birthday Keep separate from main pupil file; record transfer and receipt.
Safeguarding	Allegations against staff and volunteers	Until normal pension age or 10 years from allegation, whichever is longer	Case conclusion / employment end Subject to current KCSIE and legal advice; preserve substantiated and required records.
Safeguarding	Low-level concern records	At least employment end; review for longer retention	Employment end Follow current safeguarding policy and KCSIE.

Category	Record	Minimum retention	Trigger / notes
		where pattern or safeguarding need exists	
Health and safety	Pupil accident records	Until pupil age 25	Incident date / 25th birthday Longer if claim or investigation remains open.
Health and safety	Risk assessments and safety inspections	Current version plus 6 years	Superseded / activity end Permanent or longer for significant events or premises risks.
Health and safety	RIDDOR reports and investigation evidence	At least 3 years; 6 years preferred	Report / investigation closure Longer where child, claim or enforcement action involved.
Complaints and legal	General complaints and investigation records	Case closure + 6 years	Final response / appeal Safeguarding, employment or litigation rules may require longer.
Complaints and legal	Litigation, tribunal and legal advice files	Case closure + 6 years, or 12 years for deed-related claims	Final resolution Apply legal advice and preservation holds.
Data protection and FOI	Subject Access Requests and responses	3 years after closure	Final response Longer where complaint, claim or ICO matter arises.
Data protection and FOI	FOI/EIR requests and responses	3 years after closure	Final response Preserve significant precedent decisions longer where justified.
Data protection and FOI	Personal data breach records	6 years after closure	Incident closure Maintain full accountability record, including “not reported” rationale.
Data protection and FOI	DPIAs, ROPA and information asset registers	Current plus 6 years after superseded	Superseded / processing ends Retain evidence of decisions and review.
IT and security	User access and privileged access records	Account closure + 1 year; 6 years for privileged/admin	Account closure Align with security monitoring purpose.

Category	Record	Minimum retention	Trigger / notes
		evidence where risk warrants	
IT and security	Security, system and network logs	Typically 6 to 12 months	Log creation Set system-specific period by risk; preserve relevant logs under hold.
IT and security	Backups	According to documented backup cycle, normally no longer than necessary for recovery	Backup creation Backups are not archives; deletion occurs through rotation.
Communications	Routine administrative email and Teams messages	Delete when no longer operationally required, normally within 1 to 2 years	Message date / matter closure Move substantive decisions to the official record before deletion.
CCTV	Routine CCTV footage	Normally 30 days	Recording date Longer only for incident, request, investigation or claim.
Consent and media	Photograph/video consent and related evidence	Duration of use + 1 year	Consent withdrawal / end of use Remove published content where appropriate and practicable.

Schedule governance notes

- “Permanent” means transfer to a controlled corporate archive, not indefinite storage in operational systems.
- Where a record contains several categories, apply the longest relevant period.
- Do not destroy originals whose legal validity, evidential weight or ownership purpose depends on the original format without advice.
- Anonymised information may be retained beyond the personal-data period where re-identification is not reasonably possible.
- The Schedule must be checked against current legislation and sector guidance at least annually.

Appendix 2: Disposal and Preservation Hold Controls

A. Disposal authorisation record

Required field	Details to record
Record series	Clear description and system/location
Owner	Information Asset Owner / service
Retention rule	Schedule reference and trigger
Date range	Earliest and latest record dates
Volume	Approximate files, boxes or data size
Checks completed	No live request, audit, claim, complaint, investigation or hold
Decision	Destroy, anonymise, transfer or preserve
Authorisation	Name, role and date
Method	Shredding, certified waste, secure deletion, media destruction
Processor evidence	Certificate or confirmation where applicable

B. Preservation hold procedure

1. Identify the event and likely record scope.
2. Notify the DPO, CFOO and relevant Information Asset Owners immediately.
3. Suspend deletion, auto-deletion, mailbox deletion and destruction for in-scope records.
4. Document custodians, systems, date ranges, search terms and third parties.
5. Preserve records in a secure, read-only or otherwise controlled form.
6. Review the hold at defined intervals.
7. Release the hold only through written authorisation and reapply the normal retention rule.

Appendix 3: File Naming and Version Control

Use a consistent, meaningful convention that supports retrieval and avoids unnecessary personal data in file names.

Element	Requirement	Example
Date	Use YYYYMMDD where a date is useful	20260901
Subject	Short, meaningful title	Records Management Policy
Document type	Policy, report, minutes, contract, invoice	Policy
Version	Major.minor for controlled documents	V4.0
Status	Draft, Final, Approved	Approved
Optional unit	School or department only where useful	Central Finance

Example: 20260901 Records Management and Retention Policy V4.0 Approved.docx

- Avoid “final final” or unexplained initials.
- Do not place sensitive personal data in file names unless strictly necessary.
- Approved documents must show owner, approval body, approval date, effective date, version and review date.
- Retain the approved version and a proportionate audit trail of material changes.

Appendix 4: Sources and Supporting Guidance

The policy should be read against the latest version of each source. URLs were checked during preparation on 1 September 2026.

Department for Education, Academy Trust Handbook 2026, effective 1 October 2026
https://www.gov.uk/government/publications/academy-trust-handbook/academy-trust-handbook-2026-effective-from-1-october-2026

Department for Education, Academy Trust Handbook landing page and current versions
https://www.gov.uk/government/publications/academy-trust-handbook

Department for Education, Academies Accounts Direction 2025 to 2026
https://www.gov.uk/guidance/academies-accounts-direction

Information Commissioner's Office, Storage limitation
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/storage-limitation/

Information Commissioner's Office, Records management and security
https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/accountability/records-management-and-security/

Operational note: the Trust should maintain links to its current Financial Regulations, Scheme of Delegation, Data Protection Policy, Information Security Policy, Business Continuity Plan and safeguarding procedures in the controlled policy library.