Frank Field
Education Trust



Records Management and Retention Schedules

Policy Information:

Date prepared	October 2026
Adopted by Board	October 2026
Implementation Date	Immediate
Frequency of Review	Bi-Annually
Review Date	October 2028

Approved by CEO:

Cath Green

Approved by Chair of Board:

David Wooff

Frank Field
Education Trust

Contents

1. Statement of Intent 3
2. Legal and Regulatory Framework 3
3. Scope and Definitions 3
4. Records Management Principles 3
5. Governance and Responsibilities 4
6. Creating and Classifying Records 4
7. Pupil and Educational Records 4
8. Staff, Governance and Corporate Records 4
9. Email, Messaging and Collaborative Systems 5
10. Storage, Security and Access 5
11. Digital Continuity and Preservation 5
12. Information Rights, Disclosure and Legal Holds 5
13. Information Audit and Annual Review 6
14. Disposal, Anonymisation and Archiving 6
15. Academy Closure, Merger or Transfer 6
16. Monitoring and Review 6
Appendix 1: Retention Schedule – Pupil, Safeguarding and Education Records 7
Appendix 2: Retention Schedule – Workforce and Safeguarding Records 9
Appendix 3: Retention Schedule – Governance, Finance and Corporate Records 10
Appendix 4: Operational Records, Email and Systems 12
Appendix 5: Disposal and Preservation Log 13
Appendix 6: Schedule Interpretation Rules 13

1. Statement of Intent

Frank Field Education Trust is committed to creating and maintaining complete, accurate, accessible, and trustworthy records. Records support teaching, safeguarding, governance, accountability, efficient administration, legal rights and the history of the Trust and its academies.

This policy retains the operational areas and record categories previously adopted by the Trust while replacing outdated legal references, removing blanket assumptions and introducing clearer governance for digital records, email, preservation holds, disposal and academy closure.

Records will be kept only for as long as they are required for a documented legal, regulatory, safeguarding, contractual, evidential, operational, or historical purpose. At the end of the approved period they will be reviewed, securely destroyed, anonymised, or transferred to an appropriate archive or successor body.

2. Legal and Regulatory Framework

The policy has been reviewed against the UK General Data Protection Regulation, Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, Freedom of Information Act 2000, Environmental Information Regulations 2004, Limitation Act 1980, Equality Act 2010 and relevant employment, tax, health and safety, education, safeguarding and company law requirements.

The Trust also has regard to Keeping Children Safe in Education 2026, the School Attendance (Pupil Registration) (England) Regulations 2024, Department for Education guidance on data protection and record keeping in schools, DfE guidance for academies and academy trusts, the Academy Trust Handbook 2026, relevant accounts directions and the Information and Records Management Society school's toolkit.

The schedule is a governance tool rather than a statement that every period is fixed by statute. Where a statutory minimum applies it must be met. Where a period reflects limitation risk, safeguarding purpose, audit need or accepted sector practice, the Trust will record and periodically review the justification.

3. Scope and Definitions

This policy applies to all recorded information created, received, held, or controlled by the Trust, regardless of format or location. It includes paper, email, messaging, Microsoft 365 content, databases, management information systems, safeguarding systems, audio, video, photographs, websites, social media, logs, scanned records, backups and records held by suppliers on the Trust's behalf.

A record is information retained as evidence of an activity, decision, transaction, right, obligation or event. A retention period is the approved period for which the authoritative record must be kept. A disposal action is destruction, deletion, anonymisation, archival preservation, or transfer. A legal or preservation hold is an instruction suspending ordinary deletion because records are relevant to an actual or anticipated matter.

4. Records Management Principles

Records must be authentic, reliable, complete, usable, and protected against unauthorised alteration, loss, or disclosure. They must be captured in an approved system, named and classified consistently, linked to the appropriate pupil, employee, activity, or business function, and retained in a form that remains accessible for the required period.

The Trust will avoid unnecessary duplication. One authoritative record should be identified wherever practical. Convenience copies may be deleted when no longer needed, provided the authoritative record and any applicable preservation requirement remain protected.

Retention periods apply to content rather than media. The same record should not receive a different period merely because one copy is held electronically and another on paper.

5. Governance and Responsibilities

The Trust Board has overall accountability and will seek assurance that the Trust manages records lawfully and effectively. The Chief Executive Officer and CFOO are responsible for implementation, resourcing, and governance. Principals are responsible for local compliance and ensuring that records are transferred, reviewed, and disposed of properly.

Information Asset Owners are responsible for understanding the information within their functions, confirming the applicable schedule, controlling access, and supporting periodic review. The DPO advises on data protection, information rights, DPIAs, preservation and disposal but does not replace operational ownership. ICT staff maintain approved systems, access control, backup, recovery, and secure deletion arrangements.

All staff must create adequate records, save them in approved locations, protect them, follow retention instructions, report errors or breaches, and comply immediately with any preservation hold. Contractors must meet equivalent requirements through written contracts.

6. Creating and Classifying Records

The Trust will maintain an information asset register and an associated record of processing activities. Each significant information asset will have an owner, purpose, lawful basis where personal data is involved, location, user group, supplier where applicable, retention rule and review arrangement.

Records must be sufficiently clear to show what occurred, when, by whom, what was decided and why. Material decisions taken through informal messaging, calls or meetings must be captured in the appropriate official record where necessary.

Protective markings and access restrictions will reflect sensitivity, safeguarding risk, and business need. Special category, criminal offence, safeguarding, medical and confidential employment information will receive enhanced protection.

7. Pupil and Educational Records

The Trust will maintain pupil records so that relevant educational, safeguarding, and administrative information is accurate, accessible, and capable of secure transfer. The record will distinguish the educational file from safeguarding, complaints, medical, SEND, attendance and other specialist records where separate access controls or retention rules are required.

Safeguarding files will not be stored as an ordinary section of the general pupil file. Access will be restricted and transfer will be completed separately, securely and in accordance with Keeping Children Safe in Education. A transfer record or receipt will be retained.

Where a pupil transfers, the Trust will transfer required records securely to the new setting without unauthorised alteration. The Trust will retain only the copy or audit evidence required by the schedule or by a continuing safeguarding, complaint, legal or regulatory need.

8. Staff, Governance and Corporate Records

Personnel records will be managed as a coherent file with stricter access controls for health, equality, safeguarding, and criminal-record information. Recruitment information for unsuccessful applicants will be retained only for the approved period. Copies of DBS certificates will not normally be retained beyond six months unless a lawful exception is documented.

The Single Central Record is a live statutory safeguarding record. Historic evidence and audit records will be retained in accordance with safeguarding and employment requirements, without retaining unnecessary copies of source documents.

Signed or approved minutes of the Trust Board and principal governance committees, constitutional records, articles, schemes of delegation and records of enduring historical or legal value will be retained permanently or offered to an appropriate archive. Routine drafts and duplicate meeting packs will not be retained indefinitely.

9. Email, Messaging and Collaborative Systems

Retention follows the business value of the content, not the application in which it appears. An email, Teams message or document may be the authoritative record of a decision, safeguarding action, contract, complaint, financial transaction, or legal matter and must be captured or retained for the period applying to that business record.

The Trust will not treat every email as a record or apply a universal 12-month retention rule to substantive business records. Routine and transitory messages may be deleted under an approved lifecycle rule, but users must first capture material records in the relevant case file, business system, or approved folder.

Personal archives, local PST files, exports to personal storage and unmanaged copies are prohibited. Automatic deletion rules must be documented, communicated and capable of suspension for a legal hold, safeguarding matter, information request, complaint, investigation, or audit.

10. Storage, Security and Access

Records will be stored in approved systems with appropriate access, authentication, encryption, logging, backup, and recovery. Access will follow least privilege and will be reviewed when roles change, or access is no longer required.

Paper records containing confidential information will be held in secure storage. Records taken off site must be authorised and protected. Confidential papers or devices must not be left unattended in a vehicle merely because the vehicle is locked.

Sharing must have a lawful and authorised purpose. Consent is not required for every disclosure and must not be treated as the default lawful basis. Staff must instead follow the Data Protection Policy, privacy notices, information-sharing procedures, and safeguarding guidance.

11. Digital Continuity and Preservation

Records required for extended periods must remain readable, retrievable, and trustworthy. Information Asset Owners and ICT staff will consider file format, metadata, system dependencies, encryption keys, licensing, migration, export capability, and supplier exit arrangements.

Backup is a resilience control and is not an archive or substitute for records management. Backup retention and deletion will be documented, and restoration capability will be tested. The Trust will ensure that a record can be preserved outside its ordinary lifecycle where required.

Before a system is replaced or decommissioned, the Trust will decide which data must be migrated, archived, or deleted and will verify the outcome. Supplier contracts must support extraction, secure return or deletion and evidence of destruction.

12. Information Rights, Disclosure and Legal Holds

Records relevant to a subject access request, freedom of information request, environmental information request, complaint, grievance, disciplinary matter, safeguarding concern, audit, investigation, public inquiry, insurance claim, or actual or anticipated legal proceedings must not be altered or destroyed.

A preservation hold overrides the ordinary schedule until formally released. The responsible officer will identify the scope, notify relevant custodians, suspend automated deletion where necessary, record the hold and confirm when routine disposal may resume.

Information rights requests will be handled under the relevant Trust policy. Retention does not itself determine disclosure: exemptions, third-party rights, safeguarding considerations, and statutory restrictions must be assessed separately.

13. Information Audit and Annual Review

The Trust will review its personal data and principal information assets at least annually. The review will consider whether the information remains needed, whether the schedule is being applied, whether duplicate or unmanaged copies exist and whether systems can dispose of records securely.

The information asset register and retention schedule will be updated when a new system, process, statutory duty, or record category is introduced. Results and material risks will be reported through the Trust's governance arrangements.

14. Disposal, Anonymisation and Archiving

When the approved period expires, records will be reviewed and securely destroyed, permanently deleted, anonymised, or transferred. Disposal must be suspended where a hold or continuing need applies. An extension must have a documented reason, owner, and new review date; records must not be retained indefinitely by default.

Confidential paper will be cross-cut shredded, pulped or destroyed through an approved confidential service. Digital media will be securely sanitised or destroyed using methods appropriate to the technology and sensitivity. Third-party destruction will be supported by suitable contractual controls and evidence of destruction where appropriate.

A disposal log will record significant series destroyed, the period covered, authority, date, method, and contractor certificate where applicable. Records selected for permanent preservation will be transferred with sufficient metadata and a documented chain of custody.

15. Academy Closure, Merger or Transfer

Where an academy closes, merges or transfers, the Trust will identify the lawful successor or archive for each record series. Current pupil records and safeguarding information will be transferred securely to the appropriate new setting. Records that do not follow a pupil, required staff, premises, governance, and financial records will be transferred or retained in accordance with DfE guidance and agreed arrangements.

Governance and school-history records of permanent value will be offered to the relevant local authority archive service. No records, storage media or equipment will be abandoned when premises are vacated. The Trust will retain inventories, transfer schedules, receipts, and destruction evidence.

16. Monitoring and Review

Compliance will be monitored through information audits, system reviews, disposal logs, access reviews, breach and request handling, supplier assurance, and internal audit. Failure to follow this policy may result in management, disciplinary, contractual or safeguarding action.

This policy and its schedules will be reviewed Bi - annually and earlier where legislation, DfE guidance, safeguarding requirements, systems, or Trust practice materially change. The next scheduled review is October 2028.

Appendix 1: Retention Schedule – Pupil, Safeguarding and Education Records

Record series	Minimum / standard retention	End action and notes
Admission register	Each entry: 6 years from the date entered or under current statutory requirement if longer.	Secure deletion: retain permanent historical extract only if selected for archive.
Attendance register	Each entry: 6 years from date entered.	Secure deletion, subject to safeguarding, prosecution, or legal hold.
Pupil educational record transferred to another school	Transfer promptly to the new school; retain transfer evidence and only necessary local copy.	Secure transfer and receipt; dispose of convenience copy when no longer needed.
Pupil educational record where no onward school receives it	Date of birth + 25 years.	Review, then secure destruction or transfer to responsible authority.
Child protection / safeguarding file	Date of birth + 25 years, unless a longer safeguarding, inquiry or legal hold applies.	Secure destruction following DSL/DPO review.
Safeguarding allegations against staff	Until normal retirement age or 10 years from allegation, whichever is longer; malicious or false records handled in line with KCSIE.	Review and securely destroy when lawful.
SEND and EHC plan working records	Date of birth + 25 years as default; longer where needed for claims or statutory function.	Review and secure destruction; transfer relevant current record.
Admission appeal – unsuccessful	Case resolution + 1 year.	Secure destruction unless complaint or proceedings continue.
Exclusion / suspension records	Transfer relevant record; local copy while pupil attends + 1 year.	Secure destruction subject to appeal or legal hold.
School trip consent – no significant incident	End of trip + 3 months.	Secure destruction.
School trip / activity records involving significant incident	Date of birth + 25 years or longer where claim requires.	Secure destruction after review.
Medical administration and care plans	While current; relevant record transferred; local copy pupil leaves + 1 year.	Secure destruction unless incident or claim requires longer.
Public examination and assessment records	In line with awarding-body requirements; key results on pupil record.	Return certificates where required; secure disposal of working copies.

Record series	Minimum / standard retention	End action and notes
Images and recordings	For documented purpose and consent/lawful-basis period; review at least annually.	Delete or anonymise; preserve approved archival material separately.
Biometric data	Until pupil stops using the system or consent/authority ends, then delete promptly.	Secure deletion from live and supplier systems.

Appendix 2: Retention Schedule – Workforce and Safeguarding Records

Record series	Minimum / standard retention	End action and notes
Personnel file	Employment ends + 6 years.	Secure destruction, subject to safeguarding, pension, claim, or inquiry hold.
Unsuccessful recruitment records	Appointment decision + 6 months.	Secure destruction unless dispute requires hold.
Right-to-work evidence	Employment ends + 2 years.	Secure destruction.
DBS certificate copy	No longer than 6 months unless lawful exception recorded.	Secure destruction; retain check outcome on SCR.
Single Central Record	Current while person is engaged; retain audit/version evidence for 6 years after engagement or longer if safeguarding need.	Secure destruction following safeguarding review.
Payroll and tax records	Tax year + 6 years.	Secure destruction.
Sickness and occupational health records	Employment ends + 6 years as default; retain exposure/health surveillance records for statutory longer periods.	Secure destruction with restricted access.
Disciplinary and grievance case	Case closure + 6 years; warning status governed by HR policy.	Secure destruction subject to legal or safeguarding hold.
Safeguarding training record	Employment ends + 6 years; longer evidence may be retained where required for safeguarding claims or inquiry.	Review and secure destruction.
Pension records	Scheme requirement, normally employment ends + 6 years, with core entitlement records retained longer where necessary.	Transfer or secure destruction after review.

Appendix 3: Retention Schedule – Governance, Finance and Corporate Records

Record series	Minimum / standard retention	End action and notes
Signed Trust Board and principal committee minutes	Permanent.	Preserve; offer to archive where appropriate.
Articles, funding agreements, trust deeds, schemes of delegation	Permanent / superseded version retained permanently were evidential.	Preserve.
Board and committee agendas and supporting papers	One authoritative set: permanent where integral to decision record; otherwise, meeting + 6 years.	Archive or secure destruction.
Policies	Superseded + 6 years; permanently preserve constitutionally significant policies.	Secure destruction or archive.
Complaints	Closure + 6 years; safeguarding or negligence matters longer according to underlying record.	Review and secure destruction.
Annual accounts and accounting records	Financial year + 6 years, without prejudice to current Academy Trust Handbook and Accounts Direction.	Secure destruction after audit/hold release.
Invoices, orders, receipts, and banking records	Financial year + 6 years.	Secure destruction.
Contracts under hand	Expiry / final payment + 6 years.	Secure destruction subject to dispute or asset life.
Contracts executed as deeds	Expiry / final payment + 12 years.	Secure destruction subject to dispute or asset life.
Insurance policies and claims	Expiry + 6 years; employers' liability certificates and long-tail claims retained longer as required.	Review and secure destruction.
Title deeds, property transfer, and core building records	Permanent / duration of ownership plus transfer to successor.	Transfer or preserve.
Asbestos records	Life of premises / 40 years where exposure record requires.	Transfer with premises record or preserve.
Health and safety risk assessments	Superseded + 3 years; copy linked to incident retained with	Secure destruction.

Record series	Minimum / standard retention	End action and notes
	incident file.	
Adult accident records	Date of incident + 3 years, or longer where claim/legal hold.	Secure destruction.
Pupil accident records	Child's 21st birthday as minimum; date of birth + 25 years for significant incidents or claims.	Review and secure destruction.
RIDDOR records	Date of report + 3 years minimum.	Secure destruction subject to claim or exposure rule.
COSHH health surveillance / exposure records	40 years from last entry where regulations require.	Secure destruction after review.
Fire safety records	Current record plus 3 years; significant building safety evidence may be retained longer.	Secure destruction or transfer with premises.
Visitor logs	Date of last entry + 3 years as default; 6 years where required for investigation or contractual need.	Secure destruction.
Data breach records	Closure + 6 years.	Secure destruction after review.
FOI/EIR request files	Closure + 3 years; ICO decision or litigation files + 6 years.	Secure destruction.
Subject access request files	Closure + 3 years; complaint or litigation files + 6 years.	Secure destruction.

Appendix 4: Operational Records, Email and Systems

Record series	Minimum / standard retention	End action and notes
Routine administrative correspondence	Current year + 1 year unless content belongs to another series.	Delete after capture of substantive record.
Senior management correspondence and decision records	Creation + 6 years, or period of underlying matter.	Secure destruction or archive.
Transactional email	Retention of underlying transaction, case, or decision.	Capture in authoritative record; delete duplicates.
Team meeting minutes	Meeting + 5 years as default; longer if governance or significant decision record.	Review and secure destruction.
Newsletters and prospectuses	One archival copy permanently; working copies current year + 1 year.	Archive one copy; standard disposal of duplicates.
Information asset register / ROPA	Current version plus superseded versions for 6 years.	Secure destruction after review.
Access-control and system audit logs	Period justified by security purpose, normally 12 months; longer for incident evidence.	Automated secure deletion.
Backups	According to approved backup cycle, not used for indefinite retention.	Automated overwrite/deletion after hold checks.
CCTV footage	System-specific justified period under CCTV policy; preserved incident extracts for underlying case period.	Secure automated deletion.
Website and social-media records	Significant published content and decisions: 6 years; selected historical snapshots permanent.	Archive or delete.
General office files with no other schedule	Current year + 3 years.	Review and secure destruction.

Appendix 5: Disposal and Preservation Log

Record series / system	Date range	Authority and reason	Action / contractor	Date and evidence

Appendix 6: Schedule Interpretation Rules

The period begins from the trigger stated in the schedule, not from the date the record is found.
“Current year” means the current academic, financial or tax year appropriate to the record.
A statutory, safeguarding, contractual, audit, insurance or legal requirement overrides a shorter standard period.
A preservation hold suspends deletion until formally released.
Where a record belongs to more than one series, apply the longest justified period and document the reason.
An anonymised statistical record may be retained after personal identifiers are irreversibly removed.
Permanent means selected for continuing preservation, not left indefinitely in an unmanaged live system.
The schedule must be read with current legislation and authoritative guidance; material changes are incorporated through annual review.