CAMPFIRE EDUCATION TRUST

Records Management Policy and Record Retention Schedule

Reviewed by:	The Executive team
Date Approved:	June 2026
Review Frequency:	Every 2 Years
Next Review Date:	June 2028

Contents

---

1. Introduction

Campfire Education Trust (the Trust) recognises that effective records management is essential to supporting operational efficiency, safeguarding, accountability, legal compliance and information security.

The Trust is committed to maintaining accurate, secure and proportionate records management arrangements in accordance with statutory obligations, regulatory requirements and sector best practice.

Records provide evidence of the Trust's activities, decisions and transactions and are essential to:

- supporting effective governance;
- protecting the rights of pupils, parents, staff and the Trust;
- demonstrating accountability and transparency;
- supporting safeguarding responsibilities;
- enabling operational continuity;
- complying with legal and regulatory obligations.

This policy establishes the framework for the creation, storage, retention, archiving and secure disposal of records held by the Trust.

2. Purpose

The purpose of this policy is to:

- establish a consistent approach to records management across the Trust;
- ensure records are retained only for as long as necessary;
- support compliance with statutory and regulatory obligations;
- ensure records are stored securely and remain accessible where required;
- reduce the risks associated with excessive retention or inappropriate disposal of information;
- support efficient retrieval of information;
- protect personal data and confidential information.

3. Scope

This policy applies to:

- all Trust employees;
- trustees and governors;

- volunteers;
- contractors;
- agency workers;
- consultants;
- third parties processing information on behalf of the Trust.

The policy applies to all records created, received or maintained by the Trust in the course of carrying out its functions, regardless of format, including:

- paper records;
- electronic documents;
- emails;
- databases;
- photographs and video recordings;
- scanned records;
- CCTV footage;
- audio recordings;
- portable storage media;
- cloud-based records.

For the purposes of this policy, records are defined as all recorded information created, received or maintained by the Trust which provides evidence of activities, transactions, decisions or obligations.

4. Legal and Regulatory Framework

This policy supports compliance with:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Freedom of Information Act 2000;
- Limitation Act 1980;
- Keeping Children Safe in Education (KCSIE);
- Children and Families Act 2014;
- Employment legislation;
- Health and Safety legislation;
- IRMS Information Management Toolkit for Schools;
- Department for Education guidance;
- Information Commissioner's Office (ICO) guidance.

The Trust recognises that effective records management is fundamental to safeguarding, accountability, legal compliance and organisational resilience.

5. Roles and Responsibilities

5.1 Board of Trustees

The Board of Trustees has overall strategic responsibility for ensuring that the Trust has appropriate records management arrangements in place.

The Board will:

- delegate approval of this policy to the executive team;
- receive assurance regarding compliance;
- ensure appropriate governance oversight.

5.2 Chief Executive Officer

The Chief Executive Officer has executive accountability for the implementation of this policy across the Trust.

5.3 Headteachers

Headteachers are responsible for ensuring the effective implementation of this policy within their individual

schools.

This includes:

- ensuring staff awareness and compliance;
- ensuring records are managed appropriately;
- ensuring secure storage and disposal arrangements;
- escalating breaches or concerns.

5.4 Operations Managers / Business Managers / Office Managers

Operations, Business and Office Managers are responsible for the day-to-day management of records systems and retention processes.

Responsibilities include:

- maintaining records management systems;
- overseeing secure destruction arrangements;
- maintaining destruction logs;
- coordinating archiving arrangements;
- supporting audit and compliance activity.

5.5 Data Protection Officer

The Data Protection Officer (DPO) will:

- provide advice regarding compliance obligations;
- support monitoring and audit activity;
- advise on retention and disposal issues;
- provide guidance regarding breaches and data protection risks.

5.6 All Staff

All staff are responsible for:

- ensuring records are accurate and appropriately maintained;
- storing information securely;
- complying with retention requirements;
- disposing of records appropriately;
- reporting concerns or breaches promptly.

6. Records Management Principles

The Trust will ensure that records are:

- accurate and reliable;
- appropriately classified and organised;
- securely stored;
- accessible to authorised individuals when required;
- protected from unauthorised access, loss or destruction;
- retained only for as long as necessary;
- securely disposed of when no longer required.

The Trust will seek to minimise duplication of records where possible in order to:

- improve efficiency;
- reduce storage requirements;
- reduce the risk of data inaccuracies;
- support effective information governance.

7. Storage and Security

Records must be stored in a manner that ensures:

- confidentiality;

- integrity;
- availability;
- resilience.

Appropriate technical and organisational measures will be implemented to protect records from:

- unauthorised access;
- accidental loss;
- destruction;
- theft;
- corruption;
- misuse.

Paper records containing personal or confidential information must be stored securely.

Electronic records must:

- be stored within approved systems;
- be protected by appropriate access controls;
- be backed up appropriately;
- comply with Trust cyber security requirements.

The Trust will apply the principles of data protection by design and by default.

8. Email and Electronic Records

Emails must not be treated as personal storage systems.

Where an email constitutes a Trust record, it must be retained within the appropriate filing or records management system and managed in accordance with this policy.

Retention periods apply to the content and purpose of the email rather than the format.

Staff must ensure that:

- important emails are saved appropriately;
- duplicate emails are minimised;
- confidential information is handled securely;
- emails are deleted in line with retention requirements.

Electronic records must be managed in a way that ensures:

- accessibility;
- security;
- recoverability;
- lawful retention and deletion.

9. Retention of Records

The Trust will retain records only for as long as necessary to:

- meet legal and regulatory requirements;
- support safeguarding responsibilities;
- fulfil operational needs;
- support financial accountability;
- defend potential legal claims;
- preserve records of historical significance.

Retention periods are determined by:

- statutory obligations;
- safeguarding considerations;
- limitation periods;

- operational requirements;
- sector best practice guidance.

Retention periods may be extended where records are relevant to:

- litigation;
- complaints;
- safeguarding matters;
- insurance claims;
- investigations;
- Freedom of Information requests;
- Subject Access Requests;
- regulatory inquiries.

10. Records Retention Schedule

The Trust's detailed Records Retention Schedule forms part of this policy and must be read in conjunction with it – see Appendix A

11. Links to Existing Policies

- Freedom of Information policy
- Data Protection policy
- Other policies, legislation or regulations (including audit, equalities and diversity and business ethics) affecting the Trust

Appendix A – Records Retention Schedule

Retention Schedule Disclaimer

Retention periods contained within this schedule represent minimum retention requirements. Records may be retained longer where required for safeguarding matters, litigation, complaints, insurance claims, investigations, statutory inquiries, Freedom of Information requests, Subject Access Requests or other legitimate operational reasons.

Governance Records

Record Category	Personal Data Category	Retention Period
Articles of Association / Instrument of Government	N/A	Permanent
Governor election records	Personal Data	Election + 6 months
Governor term of office records	Personal Data	Date appointment ceases + 6 years
Governor DBS outcome records	Personal Data	Date appointment ceases + 6 years
Signed governing body minutes	Special Category Data	Permanent
Public inspection minutes	N/A	Date of meeting + 3 years
Scheme of Delegation / Terms of Reference	N/A	Until superseded

Leadership and Management

Record Category	Personal Data Category	Retention Period
SLT meeting notes	Special Category Data	Date of meeting + 3 years
General correspondence	N/A	Current year + 3 years
Policy documents	N/A	Until superseded
Safeguarding-related policies	Special Category Data	Until superseded + 3 years
Complaints records	Special Category Data	Resolution + 6 years
Visitors signing-in records	Personal Data	Current year + 6 years

Pupil Records

Record Category	Personal Data Category	Retention Period
Admissions paperwork	Special Category Data	Date of admission + 1 year
Admissions register	Personal Data	Permanent
Pupil educational record	Personal Data	Until transfer
MIS pupil records	Special Category Data	Until transfer + 6 years
SEND and EHCP records	Special Category Data	DOB + 31 years
Child protection files	Special Category Data	DOB + 25 years then review
Attendance registers	Personal Data	3 years from date of entry
Accident reports – pupils	Personal Data	DOB + 25 years
Pupil photographs	Personal Data	Duration of attendance plus limited operational period

Safeguarding Records

Record Category	Personal Data Category	Retention Period
Safeguarding concern records	Special Category Data	DOB + 25 years then review
Allegations against staff	Special Category Data	Normal retirement age or 10 years from allegation
Malicious allegations	Special Category Data	Remove from personnel file
Safeguarding training records	N/A	Date of training + 40 years

Staff Records

Record Category	Personal Data Category	Retention Period
Unsuccessful applications	Special Category Data	6 months
Contracts of employment	Personal Data	Employment ceases + 6 years

Identity verification documents	Special Category Data	Employment ceases + 2 years
DBS outcome confirmations	Special Category Data	Employment ceases + 25 years
Personnel files	Personal Data	Employment ceases + 6 years
Appraisal records	Personal Data	Current year + 6 years
Sickness records	Special Category Data	Current year + 6 years
Disciplinary records – safeguarding related	Special Category Data	Employment ceases + 25 years
Exit interview notes	Personal Data	Employment ceases + 7 years

Financial Management Records

Record Category	Personal Data Category	Retention Period
Annual accounts	N/A	Current financial year + 6 years
Budget planning records	N/A	Current financial year + 3 years
Payroll records	Personal Data	End of tax year + 6 years
Pension records	Personal Data	12 years
Invoices and receipts	N/A	Current financial year + 6 years
Contracts under seal	N/A	Final payment + 12 years
Contracts under signature	N/A	Final payment + 6 years
Employer Liability Insurance certificates	N/A	Closure of Trust + 40 years

Health and Safety Records

Record Category	Personal Data Category	Retention Period
Health and Safety policies	N/A	Life of policy + 3 years
Risk assessments	N/A	Life of assessment + 3 years
Fire logbooks	N/A	Current year + 6 years
COSHH records	N/A	Last action + 40 years
Asbestos records	N/A	Last action + 40 years
Radiation exposure monitoring	N/A	Last action + 50 years
Incident reports – adults	Special Category Data	Date of incident + 12 years
Incident reports – children	Special Category Data	DOB + 25 years
Visitor records	Personal Data	Current year + 6 years

Property and Estates Records

Record Category	Personal Data Category	Retention Period
Title deeds	N/A	Permanent
Property plans	N/A	Permanent
Lease documentation	N/A	Expiry of lease + 6 years
Premises maintenance records	N/A	Current year + 6 years
CCTV footage	Personal Data	28 days unless required for investigation

Local Authority and Government Records

Record Category	Personal Data Category	Retention Period
Secondary transfer documentation	Personal Data	Current year + 2 years
Attendance returns	Personal Data	Current year + 1 year
School census returns	N/A	Current year + 5 years
OFSTED reports	N/A	Life of report then review

Electronic Records and Communications

Record Category	Personal Data Category	Retention Period
Emails	Depends on content	In accordance with relevant record category
Cloud-based records	Depends on content	In accordance with relevant record category
Website content records	N/A	Current academic year + 3 years
Social media records	Personal Data	Current academic year + 3 years

Archiving

Certain records may be retained permanently for historical value, safeguarding significance, governance purposes, heritage interest or legal reasons. Archived records must be securely stored and maintained within an archive register.

Disposal Requirements

All records scheduled for destruction must be securely destroyed and recorded within a destruction log. No records may be destroyed where they may be relevant to litigation, safeguarding investigations, complaints, insurance claims, Freedom of Information requests, Subject Access Requests or statutory inquiries.