

Data Retention Policy

Responsible sub-committee:	Risk and Governance Committee
Linked Policies:	Data Protection Policy Subject Access Request Policy Privacy Notices Freedom of Information Policy Online safety and Acceptable Use Policies Data Breach Policy CCTV policy
Review Date:	November 2028
Target audience:	All stakeholders in the Trust
Dissemination via:	SharePoint, Trust Website

Amendments

Version	Section	Amendments	Date	Author
1.0	Not applicable	New policy	2018	Data Protection Officer
1.1	4.0	Retention Criteria, SAR and lateral flow testing added	May 2021	Data Protection Officer
1.2		Updates - Data protection in schools - Guidance - GOV.UK (www.gov.uk) which has changed some of the retention dates. Table added on SharePoint/One Drive/email retention	Nov 2023	Data Protection Officer
1.3	10	Update the below retention information to bring it in line with mStore retention. <ul style="list-style-type: none"> ▪ Maternity ▪ Paternity ▪ Payroll ▪ Pension 	March 25	Lewis Askin

Contents

1.	Introduction	1
2.	Scope of the policy	1
3.	Legal Framework	1
4.	Responsibilities.....	1
5.	Retention Criteria.....	1
6.	Management of student records	2
7.	Student Data Retention	3
8.	Staff Data Retention.....	5
9.	Governance and Management Data	7
10.	Retention of health and safety records	8
11.	Retention of financial records	9
12.	Storing and protecting information	13
13.	Disposal of data	13
14.	Monitoring and review	13

1. Introduction

We manage our records; we can comply with legal and regulatory obligations to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the trust and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

2. Scope of the policy

This policy applies to all records created, received, or maintained while carrying out the Trust's functions.

Records are defined as all those documents which facilitate the business carried out by the Trust and which are thereafter retained (for a set period) to provide evidence of its activities. These records may be created, received, or maintained in hard copy or electronically.

3. Legal Framework

The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. This policy has due regard to legislation including, but not limited to

- UK General Data Protection Regulation;
- Data Protection Act 2018; and
- the Freedom of Information Act 2000

This policy also has due regard to the following guidance [Data protection in schools - Guidance - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/data-protection-in-schools) and [IRMS Academies Toolkit - Information and Records Management Society](https://www.irmsacademies.org.uk/)

4. Responsibilities

The Trust has responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

The CEO and headteachers of each of the schools in the trust have overall responsibility for ensuring the policy is implemented correctly.

The Data Protection Officer (DPO) for the trust is also responsible for the management of records and for promoting compliance with this policy and reviewing the policy annually. The DPO is responsible for ensuring that all records are stored securely, in accordance with retention periods as outlined in this policy and that records are disposed of correctly.

The DPO is also responsible for conducting data audits, to check compliance with this policy.

5. Retention Criteria

The Trust will only retain personal data for as long as is necessary to fulfil the purposes for which it is collected. When assessing what retention period is appropriate for personal data, we take into consideration:

- The requirements of our trust and the services provided;
- Any statutory or legal obligations;
- The purposes for which we originally collected the personal data;
- The lawful grounds on which we based our processing;
- The types of personal data we have collected;

- The amount and categories of personal data; and
- Whether the purpose of the processing could reasonably be fulfilled by other means.

6. Management of student records

Student records are specific documents that are used throughout a student's life in the education system – they are passed to each school that a student attends and includes all personal information relating to them.

The following information is stored on paper or in electronic format:

- Forename, surname, preferred name/s, gender, date of birth, Unique pupil number, ethnic origin, religion and first language (if not English)
- Details of any siblings
- Emergency contact details
- Allergies including medical conditions
- Names, home addresses and telephone numbers of parent/carers
- Admission date and date of leaving
- Other agencies involved with the student
- Details of SEND
- Notes relating to major incidents and accidents involving the student
- Information about an education, health, and care plan (EHC)
- Notes indicating child protection disclosures and reports are held
- Exclusion information
- Correspondence with parents/carers/third party agencies

The following information has a shorter retention period and will therefore be stored separately:

- Consent forms for trips/visits

Much of the above information is also stored on the trust's electronic management information system (MIS) – Bromcom, secure data files on SharePoint or secure paper files. One of the schools in the trust also uses MStore to electronically store pupil and staff records.

Hard copies of disclosures and reports relating to child protection are stored in or CPOMS (safeguarding system) and (in locked cabinets at the relevant school).

7. Student Data Retention

TYPE OF FILE	RETENTION PERIOD	ACTION AT END OF RETENTION PERIOD
Personal identifiers, contacts, and personal characteristics		
Images for identification	DOB plus 25 years	Secure Disposal
Images for displays in schools	In line with consent	Secure Disposal
Images for marketing	In line with consent	Secure Disposal
Biometric data	Whilst the student is on roll at the school	Secure Disposal
Names, addresses and characteristics	DOB plus 25 years	Secure Disposal
Admissions		
Register of admissions	DOB plus 25 years	Secure Disposal
Admissions paperwork	Held by LA - date of admission or refusal plus 1 year	
Admissions appeals	Held by LA - date of admission or refusal plus 1 year	
Admissions Policy	Life of policy plus 3 years	Disposal
Students' educational records		
Primary school	Whilst the student is on roll (Unless ongoing legal action then a copy can be retained for DOB plus 25 years)	Transfer to next school
Secondary school	DOB plus 25 years	Secure Disposal
Public examination results	Added to student's record and retained in line with above	Secure Disposal
Internal examination results	Added to student's record and retained in line with above	Secure Disposal
Curriculum management		
Exam results - schools' copy	Current year plus 6 years	
SATs results	DOB plus 25 years	Secure Disposal
Published Admission Numbers	Current academic year plus 6	Secure Disposal
Census	Current academic year plus 6	Secure Disposal
Value added and contextual data	Current academic year plus 6	Secure Disposal
Student's work	Return to student at end of academic year	Secure Disposal
Exam Level Leavers	2 years from their leaving date	Secure Disposal
Medical information and administration		
Permission slips	For the duration of the period that medication is given	Secure Disposal
Medical conditions Paper Copies Electronic Copies	Transferred to next school DOB plus 25 years	Secure Disposal
Lateral Flow test results staff & students	12 months from date of the last entry in the Covid lateral flow testing log	Secure Disposal
SEND		
SEND files, reviews, and individual education plans	DOB plus 31 years (6 years from the end of being 25)	Can be longer if may be needed to defend themselves in a 'failure to

		provide sufficient education' case
EHC plans	DOB plus 31 years (6 years from the end of being 25)	Secure Disposal unless subject of a legal hold
Accessibility strategy documents	DOB plus 31 years (6 years from the end of being 25)	Secure Disposal unless subject of a legal hold
Extra-curricular activities		
Field file - information provided for a specific school trip	Until the conclusion of the trip unless there has been a major incident when it should be added to the core system and retained in line (e.g., DOB plus 25 years)	Secure Disposal
Financial information relating to school trips	Current academic year plus 6	Secure Disposal
Parental consent forms for trips where no major incident occurred	Duration of trip	Secure Disposal
Parental consent forms for trips where a major incident occurred	DOB plus 25	Secure Disposal
Catering and free school meal management		
Meal administration	Whilst the student is on roll	Secure Disposal
Meal eligibility	DOB plus 25	Secure Disposal
Child protection information		
Child protection info on pupil file	If placed on a pupil file, then the same retention period applies as the pupil file.	Secure Disposal
Child protection info in separate files	Academic year of incident plus 85 years (The IICSA report on child abuse -Oct 22 recommended 75 years with appropriate review periods). Sheffield Local authority currently recommend 85 years	Secure Disposal
Other		
Exclusions	DOB plus 25 years	Secure Disposal
Records relating to the creation and publication of the school prospectus/brochures	Current academic year	Non-secure Disposal
Newsletters and other items with short operational use	Current academic year	Non-secure Disposal
Visitors books/sign-in information	Current academic year plus 6 years	Secure Disposal
Students' absence/attendance	Attendance registers - Current academic year plus 6 years Attendance correspondence -on pupil file (see above)	

8. Staff Data Retention

TYPE OF FILE	RETENTION PERIOD	ACTION AT END OF RETENTION PERIOD
Operational		
Personnel file Application form and references, Absence monitoring, training records, exit interviews, risk assessments, occupational health, contract changes, leavers checklist	Leave date plus 6 years	Secure Disposal
Annual appraisal and assessment records	Leave date plus 6 years	Secure Disposal
Minutes of Safeguarding Supervision Meetings	Date of supervision meeting plus 6 years	Secure Disposal
Recruitment		
Unsuccessful candidate data	Date of appointment plus 6 months If the applicant has applied via an external agency, then they should consult the providers privacy statement	Secure Disposal
Successful candidate data	Relevant information added to personal file, all other information retained for 6 months (i.e., online search records kept for 6 months) If the applicant has applied via an external agency, then they should consult the providers privacy statement	Secure Disposal
Job adverts	2 years from date of advert	Disposal
DBS certificates	Should not be kept - only record that the DBS has been seen and note the number. Unless there is a risk - then a risk assessment should be performed and kept in personnel file. If the applicant has applied via an external agency, then they should consult the providers privacy statement	Secure Disposal
Staff Performance development notes and objectives	Current year + 6 years	
Proof of ID	Date of leaving plus 6 years	Secure Disposal

Right to work in the UK evidence	Date of leaving plus 6 years	Secure Disposal
Disciplinary and grievance procedures		
Child protection allegations Investigation Reports into Child Protection Allegations Against Staff Members	On Staff file until the later of normal retirement age or 10 years from the allegation. Child protection records, retention and storage guidelines (nspcc.org.uk) Allegations that are found to be malicious or false should be moved from personnel files go a secure file and retained until the later of normal retirement age or 10 years from the allegation.	Secure disposal
Sickness absence records	Current year plus 6 years due to link with sick pay and financial records	
Stage 1 & 2 Absence Formal Improvement Notice	Until the conclusion of the formal absence case plus 12 months	
Stage 1 Performance Capability Warning	Until the conclusion of the formal performance case plus 12 months Records will be retained for longer if there is any complaint, legal dispute or safeguarding issue – see separate sections.	
Final Written Performance Capability Warning	Until the conclusion of the formal performance case plus 12 months	
Level 1 Recorded Verbal Warning	Date of warning plus 6 months	Permanent Secure Disposal
Level 2 Written warning	Date of warning plus 12 months	Permanent Secure Disposal
Level 3 Final warning	Date of warning plus 18 months	Permanent Secure Disposal
Records relating to unproven incidents	Conclusion of the case, unless it is child protection (refer to child protection retention period)	Secure Disposal
Subject Access Requests		
Records relating to Subject Access Requests	Date of resolution plus 6 years	Secure Disposal of the Subject access request correspondence and copies of documents provided for the request

9. Governance and Management Data

TYPE OF FILE	RETENTION PERIOD	ACTION AT END OF RETENTION PERIOD
Board of trustees/LGB		
Articles of association and Legal documentation	Permanent	Permanent
Title deeds of properties	Permanent	Transferred to new owners if buildings are leased/sold
Plans of Trust properties	For as long as the buildings belong to the trust	Transferred to new owners if buildings are leased/sold
Leases of Trust properties	Expiry of lease plus 6 years	Secure Disposal
Records relating to the letting of school premises	Current financial year plus 6 years	Secure Disposal
Scheme of Delegation and Terms of Reference	Prior versions to be retained for 6 years	Secure Disposal
Register of Interests	6 years from the date the individual left	Secure Disposal
Trustee and Governors training records and personal records	6 years from the date the individual left	Secure Disposal
Policy documents	Life of policy plus 6 years	Secure Disposal
Complaints	Date of resolution plus 6 years. IF negligence involved then 15 years, If child protection then 40 years	Secure Disposal
Local governor elections records or parents and staff elections	Date of election plus 6 months	Secure Disposal
LGB/Board agendas and attendance records	Permanent - retained with minutes	Permanent
Approved Board minutes	Permanent	Permanent
Meeting papers/reports for LGB/Board meetings	Permanent	Secure Disposal
Minutes of SLT meetings and reports to meetings	Date of meeting plus 6 years	Secure Disposal
Headteachers correspondence	6 years	
School newsletters	Current year plus at least 1 year	
School development plan	Duration of plan plus 6 years	Secure Disposal

10.Retention of health and safety records

TYPE OF FILE	RETENTION PERIOD	ACTION AT END OF RETENTION PERIOD
Health & safety risk assessments	Duration of risk assessment plus 6 years	Secure Disposal
Accidents and injuries at work records including accident logs, RIDDOR reports	Date of last incident in book plus 6 years RIDDOR reports - incident plus 6 years Electronic records - incident plus 6 years	Secure Disposal
Accident reporting - adults	Date of incident plus 6 years	Secure Disposal
Accident reporting - students	DOB plus 25 years Limitation act for claims is 3 years after 18 th birthday. We will use 25 years so consistent with other student records.	Secure Disposal
Control of substances hazardous to health (COSHH)	Current academic year plus 40 years	Secure Disposal
Information on Asbestos risk areas - including the process on monitoring where employees are likely to encounter asbestos	Date of last action plus 40 years	Secure Disposal
Information on radiation risk areas - including the process on monitoring where employees are likely to encounter radiation. Maintenance records, safety features, PPE	Date of last action plus 50 years or until the person who the record relates is 75 (if that is greater than 50 years from the incident)	Secure Disposal
Fire precautions logbooks	Current academic year plus 6 years	Secure Disposal

11.Retention of financial records

TYPE OF FILE	RETENTION PERIOD	ACTION AT END OF RETENTION PERIOD
Maternity pay records	Date of leaving plus 6 years	Secure Disposal
Paternity pay records	Date of leaving plus 6 years	Secure Disposal
Payroll Records	Date of leaving plus 6 years	Secure Disposal
Pension contribution records	Date of leaving plus 6 years	Secure Disposal
Employers' liability insurance	Closure of school plus 40 years	Secure Disposal
Asset register	Permanent financial record	Secure Disposal
Burglary, theft, and vandalism report forms	Current academic year plus 6 years	Secure Disposal
Annual accounts	Current academic year plus 6 years	Secure Disposal
Loans and grants managed by the school	Date of last payment plus 12 years	Secure Disposal
Financial records - Invoices, receipts, requisitions, delivery notices, banking, debt collection	Current financial year plus 6 years	Secure Disposal
Contracts under seal	Last payment plus 12 years	Secure Disposal
Contracts under signature	Last payment plus 6 years	Secure Disposal
Records relating to maintenance work	Current academic year plus 6 years	Secure Disposal

TYPE OF FILE	RETENTION PERIOD	ACTION AT END OF RETENTION PERIOD
Safeguarding training	40 years (as may be required as part of an investigation)	
CCTV	<p>Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically.</p> <p>Footage may be retained for longer than 30 days, for example where there is an investigation, or a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.</p> <p>Recordings will be downloaded and stored securely in the investigation file so that it can be used as evidence if required. The retention date for this will be the same as the overall investigation (see above)</p>	

Recordings of meetings (Teams, Zoom)	Footage will be retained for 30 days unless the parties involved have agreed for it to be kept for longer (i.e., as a training video)	Deleted
Telephone calls and messages	<p>Telephone messages will be deleted after 30 days.</p> <p>Telephone calls will not be recorded</p>	

	My Documents folder on Computer drive - Staff and Students	One Drive	Emails - Inbox and Folders	Emails - Deleted Folder	Computer drives (excluding my documents)	SharePoint
Individual deletes document	Document is hard deleted and is no longer accessible by staff member - Recycle bin would need to be deleted via GPO	Document into deleted folder Individual can hard delete immediately by emptying recycle bin, the file/folder will then be moved to the secondary recycle bin for the remainder of the 93 days and only accessible by IT	Email into Delete folder for 7 days then hard deleted automatically Individual can hard delete earlier	Email into Delete folder for 7 days then hard deleted automatically Individual can hard delete earlier	Document is hard deleted and is no longer accessible by the individual	Document Into recycle bin & can be restored by the user. If the user deletes the file/folder from the recycle bin, the file/folder will then be moved to the secondary recycle bin for the remainder of the 93 days and only accessible by IT
Automatic deletion	Current staff - not forced Leavers - deleted by IT team 93 days from date of leaving	Current staff - not forced Leavers - deleted automatically after 93 days once their account has been deleted - this is permanent deletion	Current staff - not forced Leavers - deleted automatically after 93 days once their account has been deleted - this is permanent deletion	Document into Delete folder for 7 days then hard deleted automatically Individual can hard delete earlier	In line with retention policy. by the Responsible Officer (Business Manager) for the area. It is not an automatic deletion by IT.	In line with retention policy. by the Responsible Officer (Business Manager) for the area. It is not an automatic deletion by IT.

Is the document included in IT back up	<p>Document remains in back up for 60 days after permanent deletion from the server accessible only by IT</p> <p>NB it is 60 days rather than 93 as the primary system will not allow 93 days.</p>	Document remains in back up for 60 days after permanent deletion from the server accessible only by IT	Document remains in back up for 60 days after permanent deletion from the server accessible only by IT	Document remains in back up for 60 days after permanent deletion from the server accessible only by IT	Document remains in back up for 60 days (note primary IT system does not allow longer than this) - accessible only by IT	Document remains in back up for 60 days after permanent deletion from the server accessible only by IT
--	--	--	--	--	---	--

12.Storing and protecting information

Refer to Section 17 of the Data Protection Policy – Data Security

13.Disposal of data

Where disposal of information is outlined as non-secure disposal, this will be recycled appropriate to the form of the information e.g., paper recycling

Where disposal is outlined as secure disposal, this will be collected by a registered confidential waste organisation and electronic information will be scrubbed clean and where possible cut. We will obtain confidential waste certificates.

Where information must be kept permanently schools must ensure that this is kept securely in the most appropriate format.

14.Monitoring and review

This policy will be reviewed on every 3 years by the DPO and C-Suite.