Girls' Learning Trust

DATA AND RECORDS RETENTION POLICY

Approved By: Trust Board
Approval Date: October 2024

CONTENTS

1. INTRODUCTION AND AIMS

The Girls' Learning Trust ('the Trust') aims to ensure that all records, whether paper or electronic, are managed in a way that complies with legal, regulatory, and operational requirements. This Records Retention Policy is designed to govern the retention, storage, and destruction of records, ensuring that the Trust's legal obligations are met while maintaining confidentiality, security, and accessibility.

In addition to fulfilling legal and regulatory obligations, the Trust recognises the importance of maintaining accurate and comprehensive records to preserve institutional knowledge and secure future history. Proper record-keeping ensures that the Trust's achievements, decisions, and development are documented for future reference, contributing to informed decision-making, continuity, and the legacy of the Trust's educational mission.

The Trust maintains records relating to staff, pupils, parents and carers, trustees, governors, visitors, and other individuals. As a data controller as set out in the Data Protection and FOI Policy, the Trust is responsible for ensuring that all records are appropriately managed throughout their lifecycle, in line with relevant legislation.

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of:

- UK General Data Protection Regulation (UK GDPR), as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020.
- Data Protection Act 2018 (DPA 2018).
- Freedom of Information Act 2000

It is based on guidance from the Information Commissioner's Office (ICO) and the Department for Education (DfE) regarding records management and retention.

The policy also takes into account the Protection of Freedoms Act 2012 for the retention of biometric data and aligns with the ICO's guidance on the use of surveillance cameras and the management of personal information. In addition, this policy complies with the Trust's funding agreement and articles of association.

The policy should be read in conjunction with the following other relevant policies:

- Data Protection and Freedom of Information Policy
- CCTV policy
- Safeguarding and Child Protection Policy
- IT Policy
- Staff Code of Conduct

3. POLICY SCOPE

This policy applies to all Trust records, including but not limited to:

- Student records
- Personnel files
- Governance documents
- Financial records
- Health and safety documents

- Legal and contractual agreements
- Digital and electronic records (including emails, databases, and online storage)

4. RECORD RETENTION PRINCIPLES

Retention Periods

Records must be retained in line with the Trust's Retention Schedule, which is based on statutory requirements, regulatory guidance, and operational needs. The retention schedule outlines the specific retention periods for different types of records, after which they should be archived or securely disposed of.

Secure Storage

Records must be stored securely to prevent unauthorised access, damage, or loss. Paper records should be stored in locked cabinets or rooms, while electronic records must be protected with appropriate cybersecurity measures, such as password protection and encryption.

Access and Confidentiality

Access to records should be restricted to authorized personnel only. Confidential or sensitive information, especially personal data, must be handled in line with data protection laws to safeguard privacy.

5. ROLES AND RESPONSIBILITIES

Chief Executive Officer

The Chief Executive Officer has overall accountability for ensuring the policy is adhered to and implemented effectively.

Data Protection Officer (DPO)

The DPO is responsible for overseeing the implementation of this policy, ensuring compliance with data protection legislation, and providing guidance on the retention and disposal of records. Key responsibilities include:

- Overseeing the implementation of the Records Retention Policy across the Trust.
- Ensuring compliance with UK GDPR, Data Protection Act 2018, and other relevant legislation.
- Providing guidance to staff on the retention, storage, and disposal of records.
- Monitoring and auditing the Trust's records management practices to ensure adherence to the policy.
- Acting as the point of contact for any queries or concerns about records retention and disposal.

Headteacher

Each Headteacher is responsible for ensuring that records management is embedded in their school's operations and that staff are provided with appropriate training on records retention and disposal. Key responsibilities include:

- Providing leadership to ensure staff understand and comply with the Records Retention Policy.
- Ensuring that staff are trained on the principles of records retention and secure disposal.
- Liaising with the DPO and Chief Executive Officer to address any records management issues within the school.

Trust IT Team

The Trust IT Team is responsible for ensuring secure storage, archiving, and deletion of electronic

records, as well as supporting staff with technical aspects of records management. Key responsibilities include:

- Ensuring the secure storage of electronic records, including implementing encryption, password protection, and access controls.
- Managing the archiving and deletion of electronic records in line with the retention schedule.
- Assisting staff with secure electronic record deletion and technical queries related to records management.
- Monitoring and maintaining systems for automatic archiving and secure deletion.

All Staff

All Trust staff are responsible for managing the records they create or handle in accordance with this policy, including ensuring secure storage and appropriate disposal. Key responsibilities include:

- Ensuring the secure storage of both paper and electronic records to prevent unauthorized access.
- Disposing of records securely when they reach the end of their retention period, in line with the Trust's guidelines.
- Consulting with the DPO or IT Team for guidance on record retention, archiving, or secure deletion if necessary.

6. RECORD DESTRUCTION AND DISPOSAL

End of Retention Period

When records reach the end of their retention period, they must be reviewed to determine whether they should be archived for future reference or securely destroyed. The review should consider:

- Legal obligations for record retention.
- The ongoing operational, administrative, or historical value of the records.
- The relevance of the records for potential legal proceedings, audits, or inquiries.
- Whether the records contain confidential or sensitive information that requires special handling.

Once the decision is made:

- Archiving: If the records have long-term value (e.g., for historical, legal, or institutional purposes), they should be archived in a secure, accessible location, with metadata that allows for easy retrieval.
- Destruction: If records are no longer needed, they should be securely destroyed using methods appropriate to their format and sensitivity.

Methods of Disposal

Paper Records: Sensitive paper records should be shredded or placed in designated confidential waste bins or sacks for secure collection.

Electronic Records: Electronic records should be permanently deleted using appropriate IT tools to ensure they are irretrievable. Any traces of the data, including backup copies, should also be removed.

Confidential Waste

Documents containing personal, sensitive, or confidential information must be treated as confidential waste. This applies to:

- Personal data (e.g., student records, staff files, medical records).
- Information classified as confidential under Trust policies or legal requirements.

To securely dispose of confidential waste:

- Shredding: Documents should be shredded using cross-cut shredders, which offer higher security by producing smaller fragments.
- Confidential Waste Bins: Designated bins or sacks are available around the premises for the collection of confidential waste. These bins are secured and collected by approved waste disposal services.

Staff must ensure that no confidential documents are placed in general waste or recycling bins.

Electronic Deletion

Electronic records, including emails, databases, and files stored on shared drives, should be securely deleted to prevent unauthorised recovery. The deletion process should follow these steps:

- Permanent Deletion: Files should be deleted using secure deletion software that ensures data is overwritten and cannot be recovered.
- Backup and Redundancy Removal: Any copies of the deleted records, such as those stored in backup systems, should also be permanently erased.
- Consultation with IT: Staff should consult the Trust IT Team for assistance with secure deletion, particularly for complex data sets or system-wide deletions. The IT Team will ensure compliance with secure deletion standards and assist with specialized software where necessary.

Automatic Deletion

The Trust's IT systems are configured to automatically archive or delete certain records after a specified period, as outlined in the Retention Schedule. Automated processes may apply to:

- Emails stored in the Trust's email system.
- Records in cloud storage systems or shared drives.
- Logs and other system-generated data.

Key considerations:

- Notifications: Staff will be informed in advance of any scheduled automatic deletions. This provides an opportunity to review, retrieve, or retain records if needed.
- Exemptions: If records need to be retained beyond the automatic deletion date (e.g., for legal proceedings, audits, or operational needs), staff should contact the Data Protection Officer to request an exemption.
- Archiving: In some cases, records may be automatically archived instead of deleted. Archived records will remain accessible, but will be stored in a secure, less frequently accessed location.

7. EXCEPTIONS TO DELETION

Legal or Operational Needs

In some cases, records may need to be retained beyond their standard retention period due to ongoing legal proceedings, audits, or operational needs. If a record is identified for extended retention, the reasons must be documented, and the Data Protection Officer informed.

Historical or Institutional Significance

Records of historical, statistical, or institutional significance, which help preserve the Trust's history or legacy, may be archived indefinitely. Decisions to archive such records should be made in consultation with senior leadership and the Data Protection Officer.

APPENDIX ONE: DOCUMENT RETENTION PERIOD

Document / Category of Document	Reason for Retention / Relevant Legislation	Retention Period
Education and Student		
Student Records (General)	Education Act 1996; Safeguarding; Data Protection Act 2018; Academy Trust policies	Until the student reaches 25 years of age
Admissions Records (Successful Applications)	Education Act 1996; Data Protection Act 2018; Academy Trust policies	1 year after the student leaves the academy
Admissions Records (Unsuccessful Applications)	GDPR; Data Protection Act 2018; Academy Trust policies	1 year after the application process
Attendance Registers	Education Act 1996; Ofsted Requirements; Academy Trust policies	3 years after the end of the academic year
Student Files (including academic and pastoral records)	Education Act 1996; Safeguarding; GDPR; Academy Trust policies	Until the student reaches 25 years of age
Student Discipline Records	Education Act 2002; Limitation Act 1980; Academy Trust behaviour policies	25 years from the date of birth of the pupil
Examination Results (Public Exams - Academy Copy)	Education Act 1996; Data Protection Act 2018; Academy Trust policies	7 years from the student leaving the academy
Examination Results (Public Exams - Pupil Copy)	Education Act 1996; Data Protection Act 2018; Academy Trust policies	Until the student reaches 25 years of age
Internal Examination Results	Education Act 1996; Data Protection Act 2018; Academy Trust policies	5 years from the student leaving the academy
Special Educational Needs (SEN) Records	Education Act 1996; SEN Code of Practice; Academy Trust SEN policies	35 years from the date of the last entry
Child Protection Files	Keeping Children Safe in Education (KCSIE); Data Protection Act 2018; Academy Trust safeguarding policies	40 years from the date of the last entry
Looked After Children (LAC) Records	Children Act 1989; Data Protection Act 2018; Academy Trust policies	75 years from the date of birth
Records of Educational Visits	Health and Safety at Work Act 1974; Data Protection Act 2018; Academy Trust policies	14 years after the visit
Individual Education Plans (IEPs)	Education Act 1996; SEN Code of Practice; Academy Trust SEN policies	5 years from the student leaving the academy
Parental Consent Forms	GDPR; Safeguarding Requirements; Academy Trust policies	1 year after the activity ends
School Reports	Education Act 1996; Data Protection Act 2018; Academy Trust policies	25 years from the date of birth of the pupil
Student Medical Records (held by the academy)	Data Protection Act 2018; Children and Families Act 2014; Academy	25 years from the date of birth of the pupil

	Trust policies	
School Meal Registers and Free School Meals Registers	Education Act 1996; Data Protection Act 2018; Academy Trust policies	6 years from the date of entry
Records of Rewards and Sanctions	Behaviour in Schools Guidance; Data Protection Act 2018; Academy Trust behaviour policies	25 years from the date of birth of the pupil
Student Photographs (for academy use)	GDPR; Data Protection Act 2018; Academy Trust policies	Until the student leaves or consent is withdrawn
Transport Applications and Permissions	GDPR; Data Protection Act 2018; Academy Trust policies	3 years after the student leaves the academy
Homework Records	Education Act 1996; Data Protection Act 2018; Academy Trust policies	1 year after the academic year
Library Records (Borrowing history)	GDPR; Data Protection Act 2018; Academy Trust policies	Until the student leaves the academy
Pupil Premium Records	Education Act 1996; Data Protection Act 2018; Academy Trust funding policies	6 years from the end of the academic year
Student Exclusion Records	Education Act 2002; Data Protection Act 2018; Academy Trust behaviour policies	25 years from the date of birth of the pupil
Alumni Data	Data Protection Act 2018; GDPR; Academy Trust alumni engagement policies	Until consent is withdrawn
Employment and HR		
Staff Files (General)	Employment Rights Act 1996; Equality Act 2010; Data Protection Act 2018	6 years after employment ends
Recruitment Records (Unsuccessful Candidates)	Data Protection Act 2018; Equality Act 2010	6 months after recruitment process ends
Staff Training Records	Health and Safety at Work Act 1974; Data Protection Act 2018	6 years after employment ends
Staff Disciplinary Records	Employment Rights Act 1996; Data Protection Act 2018	6 years after employment ends
Staff Attendance Records	Working Time Regulations 1998; Data Protection Act 2018	3 years from the date of the record
Employee Liability Insurance	Employers' Liability (Compulsory Insurance Regulation) 1998	40 years
Financial		
Financial Records (e.g., Invoices, Payroll)	Companies Act 2006; HMRC regulations; Charities Act 2011	6 years from the end of the financial year
Budget Reports	Charities Act 2011; Financial Reporting Standards (FRS)	6 years from the end of the financial year
Bank Statements	Companies Act 2006; HMRC	6 years from the end of

	regulations	the financial year
Internal Audits	Companies Act 2006; Charities Act 2011	6 years after the audit report
Expense Claims	HMRC regulations; Companies Act 2006	6 years from the end of the financial year
Insurance Policies and Claims	HMRC regulations; Companies Act 2006	3 years after settlement
Tax and Accounting Records	Finance Act 1998; Taxes Management Act 1970	6 years from end of relevant tax year
Health and Safety		
Health and Safety Records (e.g., Accident Reports)	Health and Safety at Work Act 1974; Limitation Act 1980	3 years after the date of the incident
Risk Assessments	Health and Safety at Work Act 1974; Management of Health and Safety at Work Regulations 1999	3 years after the relevant period
Fire Safety Logs	Regulatory Reform (Fire Safety) Order 2005	6 years from the date of the last entry
COSHH Records	Control of Substances Hazardous to Health Regulations (COSHH) 2002	40 years from the date of the record
Estates and Facilities		
Building Plans and Records	Limitation Act 1980; Health and Safety at Work Act 1974	Life of the building plus 6 years
Maintenance Logs	Health and Safety at Work Act 1974; Limitation Act 1980	6 years after the date of the last entry
Leases and Property Deeds	Limitation Act 1980; Landlord and Tenant Act 1954	12 years after lease ends or indefinitely if deeds
Asbestos Management Plans	Control of Asbestos Regulations 2012	40 years from the date of the last entry
Information Technology		
IT System Logs and Records	GDPR; Data Protection Act 2018	1 year unless required for investigation
CCTV Footage	Data Protection Act 2018; GDPR	30 days unless required for investigation
Software Licenses	Contractual Obligations; Copyright Law	6 years after the end of the license period
Asset Registers (IT Equipment)	Companies Act 2006; HMRC regulations	6 years from the end of the financial year
Governance		
Governance Documents (e.g., Board Minutes)	Companies Act 2006; Charities Act 2011; GDPR	Indefinitely
Articles of Association	Companies Act 2006; Charities Act 2011	Indefinitely

Trust Policies and Procedures	Statutory Requirements; Best Practice	Until superseded plus 6 years
Trust Constitution and Incorporation Documents	Companies Act 2006; Charities Act 2011	Indefinitely
Register of Members	Companies Act 2006; Charities Act 2011	Indefinitely
Register of Directors / Trustees	Companies Act 2006; Charities Act 2011	6 years after the end of the financial year
Register of Interests	Companies Act 2006; Charities Act 2011; Academy Trust conflict of interest policy	6 years after the end of the financial year
Annual Reports and Accounts	Companies Act 2006; Charities Act 2011; Academy Trust policies	6 years from the end of the financial year
Committee Minutes and Papers	Companies Act 2006; Charities Act 2011; GDPR	Indefinitely
Trustee Declarations (e.g., fit and proper person declarations)	Charities Act 2011; Companies Act 2006; Academy Trust policies	6 years after the end of the financial year
Internal Governance Audits	Companies Act 2006; Charities Act 2011; Best Practice	6 years after the audit report
Ofsted and DfE Reports	Education Act 1996; Ofsted Requirements	Until superseded plus 6 years
Trustee and Governor Training Records	Companies Act 2006; Charities Act 2011; Best Practice	6 years after the training date
Complaints Records	Education Act 2002; Data Protection Act 2018; Academy Trust complaints policy	6 years after the resolution of the complaint
Risk Registers	Charities Act 2011; Companies Act 2006; Academy Trust risk management policy	6 years from the end of the financial year
Data Protection Impact Assessments (DPIAs)	GDPR; Data Protection Act 2018	3 years from the conclusion of the assessment
Governance Self-Evaluation Reports	Ofsted Requirements; Academy Trust policies	6 years from the end of the financial year
Trustee/Governor Meeting Attendance Records	Companies Act 2006; Charities Act 2011; Academy Trust policies	6 years from the end of the financial year
Ethical Conduct Policies and Declarations	Companies Act 2006; Charities Act 2011; Academy Trust policies	6 years after the policy is superseded
Communications with Regulators (e.g., DfE, ESFA)	Companies Act 2006; Charities Act 2011; Academy Trust policies	6 years from the end of the financial year
Contracts e.g. with suppliers or grant makers	Limitation Act 1980	Length of contract term plus 6 years
Contracts executed as deeds	Limitation Act 1980	Length of contract term plus 12 years