


## Records Retention Policy

 CITY OF LONDON ACADEMIES TRUST	<b>Approval Date:</b>	<b>Monitored By:</b>	<b>Full Review Due:</b>	<b>Review By:</b>
	11 July 2019	Trustees	July 2020	Trustees, Local Governing Bodies, employees,

## 1. Aims

The City of London Academies Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

The Trust has created this policy to outline how records are stored, accessed, monitored and disposed of, and how long data is retained for, in order to meet the Trust's statutory requirements and to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended

This policy applies to all personal data, regardless of whether it is in paper or electronic format, and seeks to provide guidance to Trust staff, trustees and governors on the handling of personal data.

## 2. Legal framework

This policy has due regard to statutory legislation including, but not limited to, the following:

- the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018)
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended)

This policy also has due regard to the guidance provided in the Information Records Management Society 'Information Management Toolkit for [AcademiesSchools](#)' 2019<sup>6</sup>

This policy will be implemented in accordance with the following Trust policies and procedures:

- Data Protection Policy
- Freedom of Information Policy

## 3. Responsibilities

The whole Trust and all employees, trustees and governors have a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

The Trustees hold overall responsibility for this policy and for ensuring it is implemented correctly.

The Local Governing Body of each Academy is responsible for promoting compliance with this policy in each Academy.

Each Academy in the Trust will have a nominated person acting as the representative of the data controller on a day-to-day basis within that Academy (the 'Academy Representative'). The representative is responsible for the implementation of the Trust Data Protection Policy within their Academy.

All staff members are responsible for ensuring that any records for which they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy and in accordance with the retention periods outlined in this policy.

#### 4. Retention of pupil records and other pupil-related information

The table below outlines the Trust's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Admissions</b>		
Register of admissions	Three years after the date on which the entry was made	Information is reviewed, and the register may be kept permanently
Secondary school admissions	The current academic year, plus one year	Securely disposed of
Proof of address (supplied as part of the admissions process)	The current academic year, plus one year	Securely disposed of
Supplementary information submitted, including religious, medical information, etc. (where the admission was successful)	Added to the pupil's record	Securely disposed of
Supplementary information submitted, including religious, medical information, etc. (where the admission was not successful)	Until the appeals process has been completed	Securely disposed of
<b>Pupils' educational records</b>		
Pupils' educational records – Primary	Whilst the pupil remains at the Academy	Transferred to the destination – if this is an independent school, home-schooling or outside of the UK, the file will be kept by the LA and retained for the statutory period
Pupils' educational records - Secondary	25 years after the pupil's date of birth	Securely disposed of
Public examination results	Added to the pupil's record	Returned to the examination board
Internal examination results	Added to the pupil's record	Securely disposed of
Child protection information held on a pupil's record	Stored in a sealed envelope for the same length of time as the pupil's record	Securely disposed of – shredded
Child protection records held in a separate file	25 years after the pupil's date of birth	Securely disposed of – shredded

<b>Attendance</b>		
Attendance registers	Last date of entry on to the register, plus three years	Securely disposed of
Letters authorising absence	Current academic year, plus two years	Securely disposed of
<b>SEND</b>		
SEND files, reviews and individual education plans	25 years after the pupil's date of birth (as stated on the pupil's record)	Information is reviewed, and the file may be kept for longer than necessary if it is required for the Trust to defend itself in a 'failure to provide sufficient education' case
Statement of SEN maintained under section 324 of the Education Act 1996 (and any amendments to the statement)	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Accessibility strategy	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
<b>Curriculum management</b>		
SATs results	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of
Examination papers	Until the appeals/validation process has been completed	Securely disposed of
Published Admission Number (PAN) Reports	Current academic year, plus six years	Securely disposed of
Valued added and contextual data	Current academic year, plus six years	Securely disposed of
Self-evaluation forms	Current academic year, plus six years	Securely disposed of

Pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Securely disposed of
<b>Extra-curricular activities</b>		
Parental consent forms for school trips where no major incident occurred	Until the conclusion of the trip	Securely disposed of
Parental consent forms for school trips where a major incident occurred	25 years after the pupil's date of birth, on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	Securely disposed of
Walking bus registers	Three years from the date of the register being taken	Securely disposed of
<b>Family liaison officers and home-school liaison assistants</b>		
Day books	Current academic year, plus two years	Reviewed, and destroyed if no longer required
Reports for outside agencies	Duration of the pupil's time at school	Securely disposed of
Referral forms	Whilst the referral is current	Securely disposed of
Contact data sheets	Current academic year	Reviewed, and destroyed if no longer active
Contact database entries	Current academic year	Reviewed, and destroyed if no longer required
Group registers	Current academic year, plus two years	Securely disposed of

## 5. Retention of staff records

The table below outlines the Trust's retention periods for staff records and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Operational</b>		
Staff personal file	Termination of employment, plus six years	Securely disposed of
Timesheets	Current academic year, plus six years	Securely disposed of
Annual appraisal and assessment records	Current academic year, plus five years	Securely disposed of
<b>Recruitment</b>		
Records relating to the appointment of a new principal/headteacher	Date of appointment, plus six years	Securely disposed of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file, and other information retained for six months	Securely disposed of
DBS certificates	Up to six months	Securely disposed of
Proof of identify as part of the enhanced DBS disclosure	After identity has been proven	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, securely disposed of
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination of employment, plus no longer than two years	Securely disposed of

Type of file	Retention period	Action taken after retention period ends
<b>Disciplinary and grievance procedures</b>		
Child protection allegations, including where the allegation is unproven	Added to staff personal file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer  If allegations are malicious, they are removed from personal files	Reviewed and securely disposed of – shredded
Oral warnings	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 1	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 2	Date of warning, plus 12 months	Securely disposed of – if placed on staff personal file, removed from file
Final warning	Date of warning, plus 18 months	Securely disposed of – if placed on staff personal file, removed from file
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related and is disposed of as above	Securely disposed of

## 6. Retention of senior leadership and management records

The table below outlines the Trust's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Board of Trustees and Local Governing Bodies</b>		
Agendas for meetings	One copy alongside the original set of minutes – all others disposed of	Securely disposed of
Original, signed copies of the minutes of meetings	Permanent	

Inspection copies of the minutes of meetings	Date of meeting, plus three years	Shredded if they contain any sensitive, personal information
Reports presented to the Board of Trustees or Local Governing Bodies	Minimum of six years, unless they refer to individual reports – these are kept permanently	Securely disposed of or, if they refer to individual reports, retained with the signed, original copy of minutes
Instruments of government, including articles of association	Permanent	
Policy documents created and administered by the Board of Trustees or Local Governing Bodies	Duration of the policy, plus three years	Securely disposed of
Records relating to complaints dealt with by the Board of Trustees or Local Governing Bodies	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes, then securely disposed of
<b>Principal/Headteacher and senior leadership team (SLT) in each Academy</b>		
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed, and securely disposed of
Reports created by the Principal/headteacher or SLT	Date of the report, plus a minimum of three years	Reviewed, and securely disposed of
Records created by the Principal/headteacher, deputy Principal/headteacher, heads of year and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed, and securely disposed of
Correspondence Principal/headteacher, deputy Principal/headteacher, heads of year and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Reviewed, and securely disposed of
Professional development plan	Duration of the plan, plus six years	Securely disposed of
School development plan	Duration of the plan, plus three years	Securely disposed of



## 7. Retention of health and safety records

The table below outlines the Trust's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below. Any information relating to medical records (e.g. sickness absence notes) should be kept in hard copy.

Type of file	Retention period	Action taken after retention period ends
<b>Health and safety</b>		
Health and safety policy statements	Duration of policy, plus three years	Securely disposed of
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely disposed of
Records relating to accidents and injuries at work	Date of incident, plus 12 years  In the case of serious accidents, a retention period of 15 years is applied	Securely disposed of
Accident reporting – adults	Date of the incident, plus six years	Securely disposed of
Accident reporting – pupils	25 years after the pupil's date of birth, on the pupil's record	Securely disposed of
COSHH	Current academic year, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years	Securely disposed of
Fire precautions <del>log books</del> <u>logbooks</u>	Current academic year, plus six years	Securely disposed of

## 8. Retention of financial records

Every company must keep adequate accounting records as defined in the Companies Act 2006.

Section 388 of the Companies Act 2006 requires that accounting records, once made, must be preserved for at least six years (public companies) or three years (private companies). It follows that where software is needed for retrieval of information in usable form, it must be available for use for the same period, as must any necessary hardware. VAT records must also be kept for at least six years.

The table below outlines the Trust's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Payroll pensions</b>		
Maternity pay records	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 (as amended)	Current academic year, plus six years	Securely disposed of
<b>Risk management and insurance</b>		
Employer's liability insurance certificate	Closure of the Academy, plus 40 years	Securely disposed of
<b>Asset management</b>		
Inventories of furniture and equipment	Current academic year, plus six years	Securely disposed of
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of
<b>Accounts and statements including budget management</b>		
Annual accounts	Current academic year, plus six years	Disposed of against common standards
Records maintained in Financial accounting software	Current academic year, plus six years	Securely disposed of
Loans and grants managed by the Academy	Date of last payment, plus 12 years	Information is reviewed, then securely disposed of
All records relating to the creation and management of budgets	Duration of the budget, plus three years	Securely disposed of
Invoices, receipts, order books and requisitions, delivery notices	Current financial year, plus six years	Securely disposed of

Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	Current financial year, plus six years	Securely disposed of
<b>Contract management</b>		
All records relating to the management of contracts under seal	Last payment on the contract, plus 12 years	Securely disposed of
All records relating to the management of contracts under signature	Last payment on the contract, plus six years	Securely disposed of
All records relating to the monitoring of contracts	Current academic year, plus two years	Securely disposed of
<b>School fund</b>		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of
<b>School meals</b>		
Free school meals registers	Current academic year, plus six years	Securely disposed of
School meals registers	Current academic year, plus three years	Securely disposed of
School meals summary sheets	Current academic year, plus three years	Securely disposed of

## 9. Retention of other Trust records

The table below outlines the Trust's retention periods for any other records held by the Trust, and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Property management</b>		
Title deeds of properties belonging to the Trust	Permanent	Transferred to new owners if the building is leased or sold
Plans of property belonging to the Trust	For as long as the building belongs to the Trust	Transferred to new owners if the building is leased or sold

Leases of property leased by or to the Trust	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of Trust premises	Current financial year, plus six years	Securely disposed of
<b>Maintenance</b>		
All records relating to the maintenance of the Academy properties carried out by contractors	Current academic year, plus six years	Securely disposed of
All records relating to the maintenance of the Academy properties	Current academic year, plus six years	Securely disposed of
<b>Operational administration</b>		
General file series	Current academic year, plus five years	Reviewed, and securely disposed of
Records relating to the creation and publication of Academy brochures and/or prospectuses	Current academic year, plus three years	Disposed of against common standards
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year, plus one year	Disposed of against common standards
Newsletters and other items with short operational use	Current academic year plus one year	Disposed of against common standards
Visitors' books and signing-in sheets	Current academic year, plus six years	Reviewed, then securely disposed of
Records relating to the creation and management of parent teacher associations and/or old pupil associations	Current academic year, plus six years	Reviewed, then securely disposed of

## 10. Storing and protecting information

- The Trust takes its Data Protection duties seriously and any unauthorised disclosure may result in disciplinary action.
- The **Academy Representative in each Academy** will undertake a risk analysis to identify which records are vital to academy management, and these records will be stored in the most secure manner.
- The **Academy Representative in each Academy** will ensure a backup of information is conducted regularly to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data. Where possible, backed-up information will be stored off the premises or in the cloud.

- Confidential paper records should be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records should not be left unattended or in clear view when held in a location with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use.
- Memory sticks should be avoided where possible and are not used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff and governors should avoid using their personal laptops or computers for Trust purposes. If personal devices are used staff and governors are expected to follow the same security procedures as for Trust-owned equipment (see ICT Acceptable Use Policyies).
- All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are sent via secure email or are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Where personal information that could be considered private or confidential is taken off the premises, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Trust premises accepts full responsibility for the security of the data.
- Before sharing data, all staff always ensure that:
  - They are allowed to share it.
  - Adequate security is in place to protect it.
  - The Trust Data Protection Policy is being followed
- All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.

- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of Trust premises containing sensitive information are supervised at all times.
- The physical security of the Trust's buildings and storage systems, and access to them, is reviewed regularly by each **site manager**. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the **Academy Representative** and extra measures to secure data storage will be put in place.
- The **Academy Representative** is responsible for continuity, and recovery measures are in place to ensure the security of protected data.
- Any damage to or theft of data will be managed in accordance with the Trust's Data Protection Policy.

## 11. Digital continuity statement

Digital data that is retained for longer than six years will be named as part of a digital continuity statement.

The **Academy Representative in each Academy** will identify any digital data that will need be named as part of a digital continuity statement.

The data will be archived to dedicated files on the Trust's servers, which are password-protected – this will be backed-up in accordance with section 10 of this policy.

Memory sticks will never be used to store digital data subject to a digital continuity statement.

On an **annual** basis, the **Trust IT Director** will review the storage methods used to ensure that new technology and storage methods are assessed and, where appropriate, added to the digital continuity statement.

The following information will be included within the digital continuity statement:

- A statement of purpose and requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats
- A description of the appropriate supported file formats for long term preservation
- A description of the retention of all software specification information and licence information
- A description of how access to the information asset is to be managed in accordance with the Trust Data Protection Policy.

## 12. Information audit

Each Academy conducts information audits on an **annual** basis against all information held by the Academy to evaluate the information the Academy is holding, receiving and using, and to ensure that this is correctly managed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018). This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Microfilm or microfiche
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information

The **Academy Representative in each Academy** is responsible for ensuring the information audit is completed. The information audit will include:

- The Academy's needs
- The information needed to meet those needs
- The format in which it is stored
- How long it needs to be kept for
- Vital records status and any protective marking
- Who is responsible for maintaining the original documents

The **Academy Representative in each Academy** will consult with staff members involved in the information audit process to ensure that the information is accurate.

### 13. Disposal of data

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

Where disposal of information is outlined as secure disposal, this will be shredded or pulped, and electronic information will be scrubbed clean and, where possible, cut.

Each Academy will keep a record of all files that have been disposed of and/or destroyed detailing WHAT information has been disposed/destroyed, WHEN, by WHOM, and HOW the information has been disposed of/destroyed.

Where the disposal action is indicated as reviewed before it is disposed, the **Academy Representative** will review the information against its administrative value – if the information should be kept for administrative value, a record will be kept of this.

If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

Where information has been kept for administrative purposes, the **Academy Representative** will review the information again after **three** years and conduct the same process. If it should be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every subsequent **three** years.

Where information must be kept permanently, this information is exempt from the normal review procedures.