Leading Learners
Multi Academy Trust

Data Protection and Retention Policy

Policy Owner:	**Liam Knowles (DPO/CFO)**
Approved by:	**Audit & Risk Committee**
Version:	**2**
Last reviewed on:	**15 October 2025**
Next review due by:	**15 October 2026**

Statement of intent

Leading Learners Multi Academy Trust is required to keep and process certain information about its staff members, pupils, their families, volunteers and external contractors in accordance with its legal obligations under data protection legislation.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, DfE, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff, trustees and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and the school believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

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

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- The Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE 'Keeping children safe in education 2025'
- Data Use and Access Act (DUAA)

This policy also has regard to the following guidance:

- ICO 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE 'Data protection in schools'
- DfE 'Generative artificial intelligence (AI) in education'

This policy operates in conjunction with the following school policies:

- Cyber-security Policy
- Freedom of Information Policy & Publication Scheme
- Subject Access Request Policy
- Child Protection and Safeguarding Policy

1.1 Applicable data

For the purpose of this policy, **'personal data'** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

'Sensitive personal data' is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
    - Racial or ethnic origin.
    - Political opinions.
    - Religious or philosophical beliefs.

- Trade union membership.
- Principles.

'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

1.2 Accountability

The school will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR and DPA, and will

provide comprehensive, clear and transparent privacy policies. The school will also provide evidence that it is complying with UK GDPR and DPA.

The trust will be able to demonstrate how data is processed as a whole across the MAT and will ensure each individual school within the trust is adhering to the same procedure and that this is being implemented and enforced in line with the wider trust policies.

Additional internal records of the school's processing activities will be maintained and kept up to date. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The school will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the Data Protection Officer (DPO), including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

2. Roles and Responsibilities

2.1 Overall responsibility for ensuring that the Trust meets the statutory requirements of all relevant data protection legislation lies with the Trustees.

2.2 The role of the DPO is to assist the school in monitoring compliance with the UK GDPR and the Data Protection Act 2018, and to advise on data protection issues.

The DPO for Leading Learners Multi Academy Trust is Mr Liam Knowles. He can be contacted at enquiries@leadinglearnersmat.co.uk. If you have any queries about this policy, please contact our DPO.

Each school also has two Designated Data Protection Leads who have day-to-day responsibility for data protection within their school:

- The Headteacher, and
- School Business Manager

3. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the school in the performance of its tasks

In accordance with Regulation 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003, as amended by the *DUAA*, the school/trust may store or access information on users' devices (e.g. through cookies or similar technologies) without prior consent where this is solely for the collection of statistical information about how the school's online services are used, and only for the purpose of improving those services.

This exception applies only where such analytical or performance cookies do not identify or profile individual users and are used exclusively in aggregate form.

The school/trust will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
    - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law

- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

The school/trust will ensure that it has privacy notices established which clearly outline the reasons why it needs to collect personal data. The privacy notice will include the following explicit details:

- Why the school/trust needs to collect personal data
- What the school/trust plans to do with the personal data
- How long the school/trust will keep the personal data
- Whether the school/trust will share the personal data with any external organisations

The privacy notice will be clear and accessible to data subjects. The privacy notice will also be reviewed by the DPO at least annually and whenever significant changes are made to how the school processes the data that it collects.

The school will ensure that any parents, pupils and staff whose personal data is included will be notified of any significant changes to the privacy notice or the way in which the school processes the data.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data. The rights are:

    - Right to rectification
    - Right to erasure ("right to be forgotten")
    - Right to restriction of processing
    - Right to data portability
    - Right to object
    - Rights in relation to automated decision-making/profiling

- The right of the data subject to raise a complaint with the ICO in relation to any processing.

The school/trust has privacy notices for the following groups, which outline the information above that is specific to them:

- Job Applicants
- Child Data
- Workforce
- Trustees and Governors

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

Where the school relies on:

- 'Performance of contract' to process a child's data, the school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the school takes responsibility for identifying the risks and consequences of the processing and puts age-appropriate safeguards in place.
- Consent to process a child's data, the school ensures that the requirements outlined in the 'Consent' section are met, and the school does not exploit any imbalance of power in the relationship between the school and the child

4. Record of Processing Activities (ROPA)

The Trust shall maintain a Record of Processing Activities (ROPA) based on a data mapping exercise.

The ROPA shall include:

• the personal data processed by the Trust;

• a description of the categories of individuals and of personal data;

• the legal basis for processing;

• the retention period for each data category; and

• the locations where the data is stored.

The ROPA shall be reviewed and updated periodically to ensure accuracy and compliance with data protection requirements.

5. Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will be conducted prior to the implementation of any generative AI tools where the processing of personal data is involved, particularly if the AI tool automates decision-making, involves profiling, or carries a risk of bias, inaccuracy, or data misuse.

A DPIA will include specific evaluation of the risks associated with AI systems, including fairness, accuracy, accountability, transparency, and security, in accordance with the DfE's 'Generative artificial intelligence in education (2025)' guidance.

DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

6. Data protection by design and default

The school will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, the school will ensure that only data that is necessary to achieve its specific purpose will be processed.

The school will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in school ICT systems.
- Implementing basic technical measures within the school network and ICT systems to ensure data is kept secure.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data

7. Processing in line with your rights

You have the right to:

- Request access to any personal data we hold about you.
- Prevent the processing of your data for direct-marketing purposes.
- Ask to have inaccurate data held about you amended.
- Prevent processing that is likely to cause unwarranted substantial damage or distress to you or anyone else.
- Object to any decision that significantly affects you being taken solely by a computer or other automated process

8. Data Security

- We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.
- We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.
- Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

9. Providing information to third parties

We will not disclose your personal data to a third party without your consent unless we are satisfied that they are legally entitled to the data. Where we do disclose your personal data to a third party, we will have regard to the eight data protection principles.

10. Subject Access Requests (SAR)

10.1.1 Data subjects may make SARs at any time to find out more about the personal data which the Trust holds about them, what it is doing with that personal data, and why. They are encouraged to make these requests by contacting the school concerned or by emailing enquiries@leadinglearnersmat.co.uk.

10.2 Responses to SARs shall normally be made within one calendar month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

10.3 Responses to SARs shall be dependent upon the terms of the UK GDPR, the DPA and associated ICO guidance.

10.4 Where a request for access to personal data is unclear, ambiguous or excessively broad, the Trust may request further information or clarification from the individual to enable it to locate the data requested. In such circumstances, the statutory response period may be paused until the necessary clarification or additional information has been received. Once the request has been clarified, the response timeframe will resume. This approach ensures that responses are accurate, proportionate and provided within the overall time limits set by data protection legislation

10.5 The Trust has defined a process for handling SARs and other data subject requests. This process is found the Trust's Subject Access Request Policy.

11. Accessing pupils' information

11.1 Pupils attending any type of school have a right of access under the DPA to their own information. This is known as the right of subject access. When a child cannot act for themselves or the child gives permission, parents will be able to access this information on their behalf.

12. Consent

12.1 In many cases, the Academy Trust can only process personal data with the consent of the individual.

12.2 In some cases, if the data is sensitive, as defined in the DPA, express consent must be obtained. Agreement to the Academy Trust processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions.

12.3 The Academy Trust has a duty of care to all staff and students and must therefore make sure that employees and those who use Academy Trust facilities do not pose a threat or danger to other users. The Academy Trust may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The Academy Trust will only use this information in the protection of the health and safety of the individual but will need consent to process this data in the event of a medical emergency, for example.

13. Processing Sensitive Information

13.1 Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the Academy Trust is a safe place for everyone. Because this information is considered sensitive under the DP Act, staff (and pupils where appropriate) will be asked to give their explicit consent for the Academy Trust to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

14. Examples of Personal Data

14.1 Definitions of personal data are highly complex, and it is difficult to define categorically. However, broadly speaking and in day-to-day use, 'personal data' is information which relates to a living, identifiable individual.

14.2 In the context of this policy and the Academy Trust's requirement to process 'personal data' as part of its duty of care and to educate its pupils, 'personal data' may include:

- school admission and attendance registers;
- pupil's curricular records;
- reports to parents on the achievements of their children;
- records in connection with pupils entered for prescribed public examinations;
- staff records, including payroll records;
- pupil behaviour records;
- personal information for teaching purposes;
- records of contractors and suppliers.

14.3 If it is necessary for the Academy Trust to process certain personal data to fulfil its obligations to pupils and their parents or guardians, then consent is not required. However, any information which falls under the definition of personal data, and is not otherwise exempt (see below), will remain confidential. Data will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this policy.

14.4 Sensitive data' may include:

- ethnic or racial origin
- political opinions
- religious beliefs
- other beliefs of a similar nature
- membership of a trade union
- physical or mental health or condition
- offence or alleged offence
- proceedings or court sentence

14.5 Where sensitive personal data is processed by the Academy Trust, the explicit consent in writing of the appropriate individual will be obtained.

15. Exemptions

15.1 There are a number of exemptions contained in the DPA. These may apply to the right of subject access or to the duty to comply with one or all of the principles.

Examples of exemptions include:

- crime and taxation
- parliamentary privilege
- research, history and statistics
- confidential references
- legal professional privilege

15.2 There are other exemptions under the DPA and would advise you seek legal advice when applying these.

16. Breach of Data Protection

If a breach occurs for example post sent to wrong address with pupil personal information, the Academy Trust must deal with a breach effectively. The breach may arise from a theft, a deliberate attack on systems, from the unauthorised use of personal data by a member of staff, or from accidental loss or equipment failure.

The Trust will ensure a **consistent, trust-wide approach** to managing data breaches through the following steps:

- **Immediate Notification**
  Any member of staff who becomes aware of a data breach, or suspects one may have occurred, must immediately notify their Headteacher**,** who will then report the breach to the DPO**.** The DPO will assess the breach and determine appropriate next steps.
- **Assessment and Recording**
  The DPO will conduct an initial ICO self-assessment to determine whether the breach is reportable to the ICO. All breaches, whether reportable or not, must be recorded centrally in the Trust's Data Breach Register.
- **Notification and Timeframes**
  If the breach is deemed reportable, the DPO will notify the ICO within 72 hours of becoming aware of the breach. Where there is a high risk to the rights and freedoms of individuals, the DPO will also ensure that affected individuals are informed without undue delay, using clear and plain language.
- **Report to Trustees**
  A termly summary of breaches and remedial actions shall be reported by the DPO to the Audit & Risk Committee.

17. Assessing the risks

The Academy Trust should assess any risks associated with the breach, as these are likely to affect the action taken once the breach has been contained. In particular, the Academy Trust will assess the adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

18. School Data

The Academy Trust is required to retain staff and student personal data for a specified period of time following their departure from an Academy within the Trust. Different categories of data will be retained for different periods of time. The relevant retention periods are noted in Annex B: RECORD RETENTION SCHEDULE.

19. Relationship with FOIA

Requests for access to personal data that are made by someone who is not the subject of that personal data are not subject access requests. These should be considered under the Freedom of Information Act 2000, but the personal information will not be disclosed if doing so will breach one of the data protection principles. The Trust has defined a process for handling SARs and other data subject requests. This process is found the Trust's Subject Access Request Policy.

20. Information Commissioner's Office

In accordance with the DUAA, the Trust has established a formal process for handling data protection–related complaints. Individuals (data subjects) who believe that the Trust has not complied with data protection legislation, including the UK GDPR, DPA 2018 or the DUAA, may lodge a complaint directly with the Trust.

The Trust will:

- Acknowledge receipt of any data protection complaint within 30 calendar days;
- Investigate the concerns raised and take appropriate steps to respond and, where necessary, to remedy any issues identified; and
- Provide a written response outlining the outcome of the investigation and any actions taken.

All complaints should be addressed to the Trust's **DPO** via:
Email: enquiries@leadinglearnersmat.co.uk
FAO: Mr Liam Knowles, DPO/CFO

If an individual remains dissatisfied after we have concluded our investigation, they may complain to the Information Commissioner's Office. Their contact details are:
Phone: 0303 123 1113 or via their live chat.
Their normal opening hours are Mon to Fri between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on Contact us | ICO.

21. About Data Retention

21.1 The corporate information, records and data of Leading Learners Multi Academy Trust is important to how we conduct business and manage employees.

21.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

21.3 This Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

21.4 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

21.5 This policy does not form part of any employee's contract of employment, and we may amend it at any time.

22. Scope of Data Retention

22.1 This policy covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

22.2 This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by employees on personal devices in accordance with our ICT and communications policy.

22.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data

22.4 The Records Retention Schedule can be found under Annex B of this Policy.

23. Guiding Principles

23.1 Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.
- We regularly monitor and audit compliance with this policy and update this policy when required.

24. Roles and Responsibilities

24.1 **Responsibility of all employees**. We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All employees must comply with this policy, the Record Retention Schedule

24.2 and any communications suspending data disposal. Failure to do so may subject us, our employees, and contractors to serious civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or dismissal. It is therefore the responsibility of everyone to understand and comply with this policy.

24.3 **Leading Learners Multi Academy Trust** is responsible for identifying the data that we must or should retain and determining, in collaboration with our Legal Team the proper period of retention. It also arranges for the proper storage and retrieval of data, co-ordinating with outside vendors where appropriate. The Trust schools will handle the destruction of their records whose retention period has expired in consultation with the Trust Leadership Team.

24.4 **Leading Learners Multi Academy Trust** along with Senior Leaders will:

- Administer the data management programme;
- Helping all staff implement the data management programme and related best practices;
- Plan, develop and prescribe data disposal policies, systems, standards, and procedures; and
- Provide guidance, training, monitoring and updating in relation to this policy.

25. Types of Data and Data Classifications

25.1 **Formal or official records.** Certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see paragraph 26 below for more information on retention periods for this type of data.

25.2 **Disposable information** consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Leading Learners Multi Academy Trust and retained primarily for reference purposes.
- Spam and junk mail.

Please see paragraph 26 below for more information on how to determine retention periods for this type of data.

25.3 **Personal data**. Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). See paragraph 34 below for more information on this.

25.4 **Confidential information belonging to others.** Any confidential information that an employee may have obtained from a source outside of Leading Learners such as a previous employer, must not, so long as such information remains confidential,

be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet. Please see our confidentiality policy or other relevant policy.

26. Retention Periods

26.1 **Formal or official records.** Any data that is part of any of the categories listed in the Record Retention Schedule contained in the Annex to this policy, must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Trusts DPO.

26.2 **Disposable information.** The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

26.3 **Personal data.** As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data.

26.4 **What to do if data is not listed in the Record Retention Schedule.** If data is not listed in the Record Retention Schedule, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Record Retention Schedule, or if you are unsure, please contact the Trust DPO.

27. Storage, Back-Up and Disposal of Data

27.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

27.2 **Destruction**. Senior Leaders are responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be co-ordinated with the help of the ICT provider.

27.3 The destruction of data must stop immediately upon notification from the Trusts Senior Leaders or the Trusts Legal Team that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see next paragraph). Destruction may begin again once the Trusts Senior Leaders or the Trusts Legal Team lift the requirement for preservation.

28. Special Circumstances

28.1 **Preservation of documents for contemplated litigation and other special situations.** We require all employees to comply fully with our Record Retention

Schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or the Trusts Senior Leaders or the Trusts Legal Team advise, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the Trusts Senior Leaders or the Trusts Legal Team determines those records are no longer needed. Preserving documents includes suspending any requirements in the Record Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

28.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact Liam Knowles or Sonia Green.

28.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

29. Breach Reporting and Audit

29.1 **Reporting policy breaches.** We are committed to enforcing this policy as it applies to all forms of data. The effectiveness of our efforts, however, depend largely on employees. If you feel that you or someone else may have breached this policy, you should report the incident immediately to a Senior Leader. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with either the Headteacher, Head of Operations, Sonia Green or our DPO. If employees do not report inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.

29.2 No one will be subject to, and we do not allow any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.

Audits. We will periodically review this policy and its procedures (including where appropriate by taking outside legal or auditor advice) to ensure we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audit

30. Training

All staff and governors will receive data protection training as part of their induction process. Data protection training will also be incorporated into ongoing professional development, particularly when there are changes to legislation, guidance, or the school's procedures. At a minimum, all staff and governors are required to complete the annual data protection training within four weeks of the expiration of their previous certificate. Training will be delivered online via The National College, and compliance will be monitored by the Headteacher, School Business Manager and Trust's HR Officer.

31. Monitoring

Trustees, on an annual basis, will review this policy unless circumstances demand an earlier review.

Annex A: DEFINITIONS

Data: all data that we hold or have control over and therefore to which this policy applies. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

Data Protection Officer: our Data Protection Officer who is responsible for advising on and monitoring compliance with data protection laws.

Disposable information: disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule.

Formal or official record: certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as formal or official records or data.

Non-personal data: data which does not identify living individuals, either because it is not about living individuals (for example financial records) or because it has been fully anonymised.

Personal data: any information identifying a living individual or information relating to a living individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special categories of personal data such as health data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Record Retention Schedule: the schedule attached to this policy which sets out retention periods for our formal or official records.

Storage limitation principle: data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed. This is referred to in the GDPR as the principle of storage limitation.

Annex B: RECORD RETENTION SCHEDULE

Leading Learners Multi Academy Trust establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

Employees should comply with the retention periods listed in the record retention schedule below, in accordance with the Leading Learners Retention Policy.

If you hold data not listed below or if you become aware of any changes that may affect the periods listed below or if you have any other questions about this record retention schedule, please contact either Liam Knowles (DPO) or Sonia Green (Head of Finance and Operations).

School Records Retention Schedule

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
1.0	**Governance**					
1.1	Instruments of government, including Articles of Association	No		Permanent	**Permanent**	
1.2	Records for all full governing body, Trustee Meetings, committee, audit and panel meetings, including: a) agendas b) any report, statutory policy (including Admissions Policy) or other paper considered at governing body/Trustees' meetings c) signed minutes	Yes*	School Governance (England) Regulations (2013)	Permanent	**Permanent**	*If meeting deals with confidential staff issues

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
					from electronic systems	
1.3	Governors/Trustees application forms - successful candidates	Yes		End of term of office + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.4	Governors/Trustees application forms - unsuccessful candidates	Yes		Date of election + 6 months	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.5	Governor/Trustees election voting forms	Yes		Date of election + 6 months	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.6	Governors/Trustees - registers and declarations of pecuniary interests	Yes		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.7	Trusts and endowments managed by the Trustees	No		Permanent	**Permanent** Retain in school whilst operationally required, then transfer to HALS	
1.8	Action plans created and / or administered by the governing body/Trustees	No		Life of action plan + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems*	
1.9	Records relating to complaints dealt with by the governing body/Trustees	Yes		Date of resolution of complaint + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems*	*It may be appropriate to review for further retention in the case of contentious disputes

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
2.0	**Management and Administration**					
2.1	Logbooks of activity in the school, maintained by teachers	Yes[1]		Permanent	**Permanent**	
2.2	School official diary	Yes[1]		Current academic year + 3 years	**Destroy** Delete securely or destroy as confidential waste	
2.3	Minutes of the senior management team and other internal administrative bodies	Yes[1]		Permanent	**Permanent**	
2.4	Reports made by the headteacher, Leadership team, teachers or management team	Yes[1]		Retain in school for date of report + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
2.5	Correspondence and general filing created by headteachers, deputy headteachers and other members of staff with administrative responsibilities	Yes[1]		Closure of file + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
2.6	Professional development plans	Yes		Closure of file + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
2.7	School development plans	No		Retain in school for closure of file + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
2.8	Employers' liability certificate	No		Permanent while school is operational	**Destroy** Destroy as confidential waste or delete securely from electronic systems once school closes	
2.9	School brochure/prospectus	No		Retain in school for current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
2.10	Circulars to staff and pupils	No		Current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
2.11	Newsletters to parents	No		Retain in school for current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
2.12	Visitors' books, signing in systems	Yes		Current academic year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
2.13	PTA (Parent Teacher Association) / old pupils' associations records	Yes		Retain in school for current academic year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

[1] Since 1 January 2005 subject access has been permitted into unstructured filing systems, including logbooks and other records created within the school, containing details about the activities of individual pupils. As such members of staff are subject to the Data Protection Act 1998.

3.0	LA (Local Authority) Data/Information					
3.1	Secondary transfer sheets (primary)	Yes		Current academic year + 2 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
3.2	Attendance returns	Yes		Current academic year + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
3.3	Circulars from the LA	No		Whilst operationally required	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
4.0	**DfE (Department for Education)**					
4.1	HMI reports	No		Permanent	**Permanent**	These are no longer produced
4.2	OFSTED reports	No		Retain in school while current; replace former report with any new inspection report	**Permanent**	
4.3	OFSTED-related papers	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
4.4	Returns to the DfE	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
4.5	Circulars from the DfE	No		Whilst operationally required	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
4.6	School census returns	Yes	Education (School Performance Information) (England) Regulations 2007	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.0	**Pupils**					
5.1	Records relating to the creation and implementation of the school's Admissions Policy	No	School Admissions Code (2014)	Retain in school for life of the policy + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.2	Admission forms: unsuccessful or withdrawn applications (including supplementary information e.g. proof of address, religion, medical conditions etc.)	Yes	School Admissions Code (2014)	a) If no appeal, 1 year from receipt b) If appealed, 1 year from resolution of case*	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*Records relating to appeals retained by Appeals Panel for 22 years from date of birth of pupil
5.3	Admission forms: successful applications	Yes	School Admissions Code (2014)	Date of admission + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Ensure that supplementary information e.g. proof of address, religion, medical conditions are added to the pupil's file
5.4	Admission registers	Yes	Education (Pupil Registration) (England) Regulations 2006	Retain in school until date of last entry in the book (or file) + 3 years	**Permanent** Transfer to HALS	If held electronically, a printout should be made at least **annually**. Any corrections made to electronic data should be clearly shown in the printout.
5.5	Attendance registers	Yes	Education (Pupil Registration) (England) Regulations 2006	Date of register + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.6	Pupil absence letters / leave forms / correspondence relating to authorised absence	Yes		Date of absence + 2 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.7	Absence books	Yes		Current year + 6 years from last entry in book	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.8	Telephone message books for recording absences (sickness) or changes to pick up arrangements, etc.	Yes		Current year + 6 years from last entry in book	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.9	Child protection files • **Primary**	Yes	DfE 'Keeping Children Safe in Education' Annex B, p.61	Retain while the pupil remains at the primary school*	Follow guidelines in 5.13 for pupils transferring to another school	*CP information must be kept separate from the main pupil file. Where children leave the school or college ensure their child protection file is transferred to the new school or college as soon as possible. This should be transferred separately from the main pupil file, ensuring secure transit. Confirmation of receipt should be obtained.

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.10	Child protection files • **Secondary**	Yes	DfE 'Keeping Children Safe in Education' (2016), Annex B, p.61	Date of birth of pupil + 25 years*	**Destroy or as below** If the child leaves the school: follow guidelines in 5.13 for pupils transferring to another school If the retention period is reached: destroy as confidential waste or delete securely from electronic systems	*CP information must be kept separate from the main pupil file. Both the educational record and CP information must be retained for 25 years from DOB. Where children leave the school or college ensure their child protection file is transferred to the new school or college as soon as possible. This should be transferred separately from the main pupil file, ensuring secure transit. Confirmation of receipt should be obtained.
5.11	Pupil's educational record (pupil file) **Pupils with Special Educational Needs (SEN)** • **Primary**	Yes	Retain while pupil remains at the primary school	Retain while the pupil remains at the primary school*	Follow guidelines in 5.13 for pupils transferring to another school	Includes: • SEN reviews • Individual Education Plans (IEPs) / pupil profiles • Health questionnaires • Parental consent forms • Health care plans • Records of medicine administered

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.12	Pupil's educational record (pupil file) **Pupils with Special Educational Needs (SEN)** • **Secondary**	Yes		Date of birth of pupil + 22 years*	**Destroy or as below** If the child leaves the school: follow guidelines in 5.13 for pupils transferring to another school If the retention period is reached: destroy as confidential waste or delete securely from electronic systems	*Unless child protection applies, in which case retain for 25 years from DOB; see 5.10. Includes: • SEN reviews • Individual Education Plans (IEPs) / pupil profiles • Health questionnaires • Parental consent forms • Health care plans • Records of medicine administered • Work experience agreements
5.13	Pupil's educational record (pupil file) **All other pupils** • **Primary**	Yes	The Education (Pupil Information) (England) Regulations 2005	Retain while the pupil remains at the primary school, then: a) Pupil transfers to a known Local Authority primary or secondary school in same area	**The file should follow the pupil when he/she leaves primary school:** a) Send pupil record to new school	Includes: • Health questionnaires • Parental consent forms • Health care plans • Records of medicine administered

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
				b) Pupil transfers to a known Local Authority or independent primary / secondary school which is another county within the UK, or transfers to an independent school within the Local Authority	b) Send pupil record to new school, retaining a copy or summary until pupil is 22 years old, then destroy confidentially or delete securely	
				c) Pupil transfers to a known primary / secondary school outside of the UK	c) Send a copy of pupil record to new school, retaining original pupil record until pupil is 22 years old, then destroy confidentially or delete securely	
				d) Pupil transfers to an unknown school	d) Retain pupil file until pupil is 22 years old, then destroy confidentially or delete securely	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.14	Pupil's educational record (pupil file) **All other pupils** • **Secondary**	Yes	Limitation Act (1980)	Date of birth of pupil + 22 years*	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*Unless child protection applies, in which case retain for 25 years from DOB; see 5.10. Includes: • Health questionnaires • Parental consent forms • Health care plans • Records of medicine administered • Work experience agreements
5.15	Pupil's educational record (pupil file) • Deceased pupils	Yes		Date of death + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.16	Images of pupils - signed consent forms by parent / guardian	Yes		Date of signing + 5 years; or at end of project; or when pupil leaves the school	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Images should not be reused outside of the time period or for other projects other than that specified on the form
5.17	Activity / visit / trip consent forms - signed by parent or guardian where no incident occurs	Yes		Date of event + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.18	Activity / visit / trip consent forms - signed by parent or guardian where a major incident occurs	Yes	Limitation Act 1980	Date of birth of child involved in incident + 22 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	**Important:** consent forms for ALL pupils for an event where a major incident occurs must be retained, not just that of the child involved
5.19	Behaviour Logs	Yes		Retain while the pupil remains at the primary school	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.20	SATS papers (completed)	Yes	Department for Education (DfE) recommendation	Current year + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.21	SATS results for individual pupils	Yes			Add to the main pupil file and follow retention period for 5.14	
5.22	Internal and external examination papers (completed)	Yes		Current academic year + 6 years or until any appeals / validation process is complete	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.23	Internal and external examination results for individual pupils	Yes			Add to the main pupil file and follow retention period for 5.14*	*Uncollected GCSE and A Level certificates should be returned to the relevant examination board
5.24	Examination results - summaries or other statistical information created by the school	Yes		Current academic year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
5.25	Any other records created in the course of contact with pupils maintained for teachers' own use (i.e. NOT part of the educational record)	Yes		Current academic year + 3 years	**Review** Review by school and EITHER allocate further retention period OR destroy as confidential waste or delete securely from electronic systems	
5.26	Annual parents' meetings	Yes		Permanent	**Permanent**	
6.0	**Curriculum**					
6.1	Curricula records	No		Whilst operationally required	**Destroy** Destroy as confidential waste or delete securely from electronic systems	May include: • curriculum development records • lesson plans • syllabuses • schemes of work • timetables • mark books • records of homework set

7.0	**Human Resources**					
7.1	Interview notes and recruitment records (including pre-employment vetting information) • unsuccessful candidates	Yes		Date of interview + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Includes: • proof of identity • proof of right to work in the UK
7.2	Interview notes and recruitment records (including pre-employment vetting information) • successful candidates	Yes		Follow retention period for 7.4	All recruitment information to be added to staff personnel file, except DBS checks (for DBS see 7.3)	
7.3	Pre-employment vetting information • successful candidates' DBS checks*	Yes	DfE 'Keeping Children Safe in Education' guidance (regularly updated)	Maximum of date of check + 6 months	**Destroy** Destroy as confidential waste or delete securely from electronic systems by the designated member of staff	*Formerly CRB checks Schools are not required to retain copies of DBS certificates. If the school chooses to do so, the copy must NOT be retained for longer than 6 months
7.4	Staff files (main personnel file)	Yes	Limitation Act (1980)	End of employment + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
7.5	Staff annual appraisal / assessment records	Yes		Current appraisal year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.6	Staff timesheets	Yes	Financial regulations	Current academic year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	May be held on SAP
7.7	Staff sickness records, excluding ill-health referrals (self-certification, doctor's certificates)	Yes		Current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.8	Staff sickness records • ill health referrals	Yes	Limitation Act (1980)		Add to main personnel file and follow retention period for 7.4	
7.9	Staff maternity and paternity pay records	Yes	Statutory Maternity Pay Regulations (1986) (as amended)	Current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.10	Disciplinary proceedings* • warnings	Yes			Add to main personnel file and follow retention period for 7.4	*For child protection / safeguarding disciplinary proceedings, see 7.13
7.11	Disciplinary proceedings* • substantiated or unsubstantiated	Yes		a) outcome letter: end of employment + 7 years b) all other records: close of case + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*For child protection / safeguarding disciplinary proceedings, see 7.13

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
7.12	Disciplinary proceedings* • false or malicious	Yes		a) outcome letter: end of employment + 7 years b) all other records: shred at close of case	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*For child protection / safeguarding disciplinary proceedings, see 7.13
7.13	Disciplinary proceedings* • safeguarding / child protection related	Yes	DfE 'Keeping Children Safe in Education' guidance (regularly updated)	Until normal pension age, or for 10 years from date of allegation, whichever is longer	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*Including where the allegation is unsubstantiated
7.14	Records of industrial tribunals, disciplinary panels, appeals	Yes	Limitation Act 1980 can apply		a) outcome letter: add to personnel file and follow retention period for 7.4 b) all other records: shred 7 years from end of process	
7.15	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		End of employment + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.0	**Health and Safety (H&S)**					
8.1	Health and safety policies	No		Life of policy + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
8.2	Risk assessments: general	No	Limitation Act (1980)	Date of risk assessment + 7 years (update regularly)	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.3	Risk assessments: exposure to noise, vibration, lead, asbestos, chemicals and biohazards (including COSHH)	No	Control of Substances Hazardous to Health Regulations (2002), Regulation 11 Control of Asbestos at Work Regulations (2012), Regulation 19	Date of risk assessment + 40 years (update regularly)	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.4	Risk assessments: exposure to radiation	No	Ionising Radiation Regulations 1999 (SI 1999/3232)	Date of risk assessment + 50 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.5	Accident reporting: adults a) accident books b) Reportable injury forms c) Accident investigation records	Yes	Social Security (Claims and Payments) Regulations (1979), Regulation 25 Social Security Administration Act (1992), Section 8. Limitation Act (1980)	(a) Current year + 3 (b) Current year + 3 (c) Current year + 3	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Since April 2016 accident reporting has been completed online, and all copies are held electronically

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
8.6	Accident reporting: children a) accident books b) Reportable injury forms c) Accident investigation records	Yes	Social Security (Claims and Payments) Regulations (1979), Regulation 25 Social Security Administration Act (1992), Section 8. Limitation Act (1980)	(a) Keep books until youngest child entered has reached age 22 (b) Date of birth of child + 22 years (c) Date of birth of child + 22 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Since April 2016 accident reporting has been completed online, and all copies are held electronically
8.7	Violent incident reporting (VIR)	Yes	Limitation Act (1980)	Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.8	Physical intervention forms	Yes		Date of birth of child + 22 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.9	Fire precaution logbooks (e.g. records of drills and tests)	No	Limitation Act (1980)	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.10	Accessibility plans	Yes	Equalities Act (2010)	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
8.11	Health and safety training records	Yes		While current + 6 years, unless records apply for limited period (e.g. First Aid Certificates)	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.12	Maintenance records for any work equipment, including ladders, trollies, PPE, PAT etc.	No		Current year + 10 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.13	Health and safety inspection records, including: • site inspections • playground inspections	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.0	**Finance**					
9.1	Annual accounts	No		Retain in school for current year + 6 years	**Transfer to archive** Offer to HALS to review for historic interest	
9.2	Annual budget and background papers	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.3	Budget reports and budget monitoring records	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
9.4	Records covered by various financial regulations Including: invoices, receipts, order books, requisitions, delivery notices, petty cash records, records relating to the collection and banking of monies, records relating to the identification and collection of debt	No	Financial regulations	Current financial year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.5	Copy orders	No		Current year + 2 years, or current year + 6 years if included with delivery notes, invoices and receipts, etc.	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.6	Loans and grants managed by the school	No	Financial regulations	Date of last payment on loan + 12 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.7	School Fund records Including: cheque books, paying-in books, ledgers, invoices, receipts, bank statements, journey books	No	Financial regulations	Current financial year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.8	Contracts: under seal		Limitation Act (1980)	Contract completion date + 13 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
9.9	Contracts: under signature		Limitation Act (1980)	Contract completion date + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.10	Contracts: monitoring records			Current year + 2 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.11	Free school meals records	Yes	Financial regulations	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.12	School meals registers	Yes		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.13	School meals summary sheets	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.14	Applications for free school meals, travel, uniforms etc.	Yes	Financial regulations	Whilst child at school or current year + 6 years, whichever is the longest	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.15	Payroll records where school administers own payroll	Yes	Financial regulations	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
9.16	Records relating to individuals' pension details	Yes	Financial regulations	End of employment + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.0	**Property**					
10.1	Title deeds of all properties belonging to the school	No		Permanent	**Permanent**	
10.2	Plans of all properties belonging to the school	No		Permanent	**Permanent**	
10.3	Leases of properties leased by or to the schools	No		Expiry of lease + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.4	Records relating to the letting of school premises	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.5	Burglary, theft and vandalism report forms			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.6	All records relating to the maintenance of the school, including maintenance log books	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
10.7	Inventories of equipment and furniture			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.8	Insurance papers			While current	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

11.0	**Miscellaneous**					
11.1	Photo albums			While useful	**Transfer to archive**	
11.2	Audio and video recordings			While useful	**Transfer to archive**	