L.E.A.D. Academy Trust
Lead • Empower • Achieve • Drive

L.E.A.D. ACADEMY TRUST

United Kingdom General Data Protection Regulation Policy

Policy/Procedure management log

Document name	GDPR Policy
Trust approval	December 2025
Date approved by AGB	Spring 2026
Date of review	**January 2027**

Contents

1. Introduction to this Policy

1.1 The Board of Directors and management of L.E.A.D. Academy Trust ("we", "us", "the Trust"), located at 5a The Ropewalk, Nottingham, NG1 5DU are committed to ensuring the confidentiality and security of the Personal Data held by the Trust. We are committed to ensuring compliance with all relevant UK laws in respect of Personal Data, and the protection of the "rights and freedoms" of individuals whose information L.E.A.D. Academy Trust collects and processes in accordance with the UK General Data Protection Regulation (UK GDPR).

1.2 "Artificial Intelligence (AI)" refers to systems or software that perform tasks typically requiring human intelligence, such as learning, reasoning, problem-solving, and decision-making, including machine learning, natural language processing, and automated decision-making.

1.3 L.E.A.D Academy Trust has implemented this data protection policy to set out how we will comply with the UK GDPR and other relevant policies such as the Information Security Policy (GDPR DOC 5.2), along with connected processes and procedures.

1.4 The UK GDPR and this policy apply to all of L.E.A.D. Academy Trust's Personal Data Processing functions, including those performed on students' and prospective students, customers', clients', applicants', employees', suppliers' and partners' Personal Data, and any other Personal Data the organisation processes from any source.

1.5 L.E.A.D. Academy Trust has established objectives for data protection and privacy, which are documented in PIMSL and GDPR Objectives Record.

1.6 L.E.A.D Academy Trust's Data Protection Officer/GDPR Owner is responsible for reviewing the register of Processing annually in the light of any changes to L.E.A.D. Academy Trust's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register must be available on the supervisory authority's (such as the Information Commissioner's Office) request.

1.7 It is important that all personnel at L.E.A.D Academy Trust supports our commitment to ensuring compliance with Data Protection Laws, and protecting the Personal Data we hold. This policy applies to all employees and staff of L.E.A.D. Academy Trust, including permanent, temporary, outsourced suppliers and volunteers. It is therefore important that you read and understand this policy and ensure you take steps to comply when Processing Personal Data on behalf of the Trust.

1.8 Any breach of the UK GDPR or this this policy will be dealt with under L.E.A.D. Academy Trust's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

1.9 Partners and any third parties working with or for L.E.A.D. Academy Trust, and who have or may have access to Personal Data, will be expected to have read, understood

and to comply with this policy. No third party may access Personal Data held by L.E.A.D. Academy Trust without having first entered into a data confidentiality agreement, which can be found on the L.E.A.D. Academy Trust portal. This imposes on the third-party obligations no less onerous than those to which L.E.A.D. Academy Trust is committed, and which gives L.E.A.D. Academy Trust the right to audit compliance with the agreement. This is vital to ensure we continue to protect the Personal Data we hold and maintain compliance.

1.10 L.E.A.D Academy Trust reserves the right to amend this policy from time to time, as needed. If you have any queries about this policy or how to comply, please contact our Data Protection Officer/GDPR Owner, by email using sars@leadacademytrust.co.uk

2. Key terms used in this Policy

2.1 Within this Policy, we use a number of terms that, in some cases, are drawn from UK data protection legislation. We have set out below the key definitions referred to in this policy and what they mean:

"***Controller***" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"***Data Protection Laws***" means the Data Protection Act 2018 and the UK General Data Protection Regulation ("UK GDPR").

"*Data Subject*" is a term used in data protection legislation, and it means the individual to whom the Personal Data relates. For simplicity, within this policy we sometimes refer to these people as "individuals".

"***Data Subject Consent*"** means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data.

"***Personal Data***" means any information relating to an identified or identifiable natural person ('the Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to a piece of information whether on its own, or when combined with other information held by us. Examples of Personal Data which the Trust may use or hold includes:

- a name, address, telephone number, email address and other contact details;
- an identification number;
- location data;
- bank account details;
- gender, sex or religion of an individual;
- health and disability information;
- logon credentials;

- job titles, CV, employment history and educational qualifications; and
- photographs, CCTV, video footage or audio recordings.

"***Special Category Personal Data***" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning an individual's sex life or sexual orientation.

"***Processing***" means any activity which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller

"***Profiling***" means any form of automated Processing of Personal Data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the Data Subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

"***Personal Data Breach***" means a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. There is an obligation on us to report Personal Data breaches to the supervisory authority and where the breach is likely to adversely affect the Personal Data or privacy of the Data Subject. It is therefore vital that you remain vigilant and notify our Data Protection Officer as soon as possible if you suspect any breach or unauthorised third party access has taken place. If you are ever unsure, it is always best to report an incident.

3. L.E.A.D Academy Trust's personal information management system (PIMS)

3.1 To support and reinforce L.E.A.D Academy Trust's compliance with the UK GDPR, the Board of Directors has approved and supported the development, implementation, maintenance, and continual improvement of a documented personal information management system ('PIMS'). The PIMS allows the Trust, and its staff, to ensure the Personal Data we hold is kept secure, and helps us to identify and manage any risk to that data. It allows us to ensure our ongoing compliance with data protection legislation, and promotes trust and confidence in L.E.A.D Academy Trust in managing and holding individual's Personal Data.

3.2 All employees and staff of L.E.A.D. Academy Trust and any other external parties identified by PIMS are expected to comply with this policy and with the PIMS that

implements this policy. Appropriate training on the systems and compliance with this policy will be issued to all employees and staff and certain external parties as and when required. The consequences of breaching this policy are set out in L.E.A.D. Academy Trust's disciplinary policy, and for the case of third parties, in the relevant contracts and agreements with third parties. If you feel that you need additional training, please let the Data Protection Officer know.

3.3 In determining its scope for compliance with BS 10012:2017 and the UK GDPR, L.E.A.D. Academy Trust considers:

- any external and internal issues that are relevant to the purpose of L.E.A.D. Academy Trust and that affect its ability to achieve the intended outcomes of its PIMS;
- specific needs and expectations of interested parties that are relevant to the implementation of the PIMS;
- organisational objectives and obligations;
- the organisations acceptable level of risk; and
- any applicable statutory, regulatory, or contractual obligations.

3.4 L.E.A.D. Academy Trust's objectives for compliance with the UK GDPR and a PIMS:

- are consistent with this policy;
- are measurable;
- take into account UK GDPR and BS 10012:2017 privacy requirements and the results from risk assessments and risk treatments;
- are monitored;
- are communicated; and
- are updated as appropriate.

These objectives are documented by L.E.A.D. Academy Trust in the PIMS and UK GDPR Objectives Record.

3.5 In order to achieve these objectives, L.E.A.D. Academy Trust has determined:

- what will be done;
- what resources will be required;
- who will be responsible;
- when it will be completed; and
- how the results will be evaluated.

3.6 If you have any queries about L.E.A.D Academy Trust's PIMS, please contact our IT Team at ictsupport@leaditservices.co.uk.

4. L.E.A.D Academy Trust's role in Processing Personal Data and the role of the Data Protection Officer

4.1 L.E.A.D. Academy Trust is a Controller and Processor under the UK GDPR. This means that in some instances, we are Processing Personal Data for a means and purpose determined by the Trust. In other circumstances, we are Processing some Personal Data on behalf of another Controller and doing so under, and in accordance with their instructions. The governing board has overall responsibility for ensuring that our schools within the Trust comply with all relevant data protection obligations.

4.2 Senior management, and all those in managerial or supervisory roles throughout L.E.A.D. Academy Trust, are responsible for developing and encouraging good information handling practices within L.E.A.D. Academy Trust; further details of responsibilities are set out in individual job descriptions.

4.3 The L.E.A.D Academy Trust's Data Protection Officer ("DPO") /GDPR Owner is accountable to the Board of Directors of L.E.A.D. Academy Trust for the management of Personal Data within the Trust, and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- Development and implementation of the UK GDPR, as required by this policy; and
- Security and risk management in relation to compliance with this policy.

4.4 The DPO has been considered by the Board of Directors to be suitably qualified and experienced, and has been appointed to take responsibility for L.E.A.D. Academy Trust's compliance with this policy on a day-to-day basis. In particular, they have direct responsibility for ensuring that L.E.A.D. Academy Trust complies with the UK GDPR, as do Manager/Executive (generic/line)'s in respect of data Processing that takes place within their area of responsibility.

4.5 If you have any queries or require any clarification as to any aspect of data protection compliance the DPO/GDPR Owner is the first point of call. It is the responsibility of all employees and staff who process Personal Data to ensure compliance with data protection legislation, and to raise any concerns to the DPO/GDPR Owner immediately.

4.6 L.E.A.D. Academy Trust's Training Policy (GDPR DOC 1.1) sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of L.E.A.D. Academy Trust generally.

5. The rules for Processing Personal Data

All Processing of Personal Data must be conducted in accordance with the data protection principles as set out in Article 5 of the UK GDPR. L.E.A.D. Academy Trust's policies and procedures are designed to ensure compliance with these principles.

5.1 Personal Data must be processed lawfully, fairly and transparently

L.E.A.D Academy Trust must ensure that for all Personal Data we process, we have a lawful basis for doing so. There are a number of lawful basis that are likely to be relevant to our Processing, including:

- The Processing of the individual's Personal Data is necessary to perform a contract with that individual or to take steps at the request of the individual before entering into a contract;
- The Processing is necessary to comply with a legal obligation to which the Trust is subject;
- The Processing is necessary in order to protect the vital interests of an individual;
- The Processing is necessary to perform a task carried out in the public interest, or in the exercise of official authority vested in us;
- The Processing is necessary for our legitimate interests, provided those interests are not overridden by the individual's interests, right or freedoms. Individuals have a right to object to our Processing of their Personal Data when we are relying on this lawful basis for that Processing; or
- The individual has given his or her consent to the Processing, or in the case of a child below the age of 13 years old (or a child over the age of 13 that does not have the capacity to provide consent), their parent or guardian with parental responsibility over the child has given their express consent. Data Subject Consent must be freely given, specific, informed and an unambiguous indication of the individual's wishes and made by a clear or affirmative action signifying agreement to the Processing in order to be valid. Consent obtained under duress or on the basis of misleading information will not be a valid basis for Processing. Data Subjects can withdraw their consent at any time, and we will ensure it is easy for them to do so. If someone contacts you to withdraw their consent please let the DPO/GDPR owner know immediately.

An extra layer of rules apply when we process Special Category Personal Data, and in addition to one of the lawful bases above, we must also have an additional justification for the Processing such as explicit consent or if it is necessary for our legal obligations in respect of social or employment security purposes.

In most instances, consent to process personal and sensitive data is obtained routinely by L.E.A.D. Academy Trust using standard consent documents from L.E.A.D. Academy Trust Portal. e.g. when a new client signs a contract, or during induction for participants on programmes.

Where L.E.A.D. Academy Trust provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16.

L.E.A.D. Academy Trust use CCTV in various locations around school sites to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

We must also ensure that the Processing is fair, and that we make available to the Data Subject information as to whether their Personal Data was obtained directly from them, or from other sources. Individuals trust us with their Personal Data, and therefore it is vital we are using it in a way that is lawful and transparent. Our data privacy notice's should be clear and inform individuals why their Personal Data is collected and what it is used for. Our policy ensures that certain prescribed information is provided to the individual including the purposes of Processing, the retention period of storing the data and the Data Subject's rights.

L.E.A.D. Academy Trust's Privacy Notice Procedure is set out in GDPR DOC 2.1 and the Privacy Notice is recorded in GDPR REC 4.1. A link to our Privacy Notices can be found at the trusts website www.leadacademytrust.co.uk.

5.2 **Personal Data can only be collected for specific, explicit and legitimate purposes**

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of L.E.A.D. Academy Trust's GDPR Register of Processing. Privacy Procedure GDPR DOC 2.1 sets out the relevant procedures.

5.3 **Personal Data must be adequate, relevant and limited to what is necessary for Processing**

The DPO/GDPR Owner is responsible for ensuring that L.E.A.D. Academy Trust does not collect information that is not strictly necessary for the purpose for which it is obtained (refer to DPIA Tool GDPR REC 4.4 for the data flow/mapping).

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the DPO/ GDPR Owner.

The DPO/ GDPR Owner will ensure that, on an annual basis all data collection methods are reviewed by Internal Audit to ensure that collected data continues to be adequate, relevant, and not excessive (Data Protection Impact Assessment Procedure GDPR DOC 2.4 and DPIA Tool GDPR REC 4.4).

All employees/staff of L.E.A.D Academy Trust must ensure that Personal Data is not processed in a way that goes beyond the purpose in which it is held.

5.4 **Processing personal data with AI**

Where L.E.A.D. Academy Trust uses AI systems to process personal data, such processing will be subject to the same lawful bases and transparency requirements as other forms of processing.

The Trust will ensure that individuals are informed when their data is processed by AI, especially where automated decision-making or profiling occurs.

Any use of AI that involves automated decision-making with legal or similarly significant effects will be subject to a Data Protection Impact Assessment (DPIA) prior to implementation.

5.5 **Data Accuracy**

It is important that we ensure that all Personal Data we hold is accurate, and we will take reasonable steps to ensure that any inaccurate data is rectified or erased as soon as possible. Data must be reviewed and updated as necessary, and it should not be kept unless it is reasonable to assume that it is accurate.

The DPO/GDPR Owner is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is also the responsibility of the Data Subject to ensure that data held by L.E.A.D. Academy Trust is accurate and up to date. Completion of a registration or application form by a Data Subject will include a statement that the data contained therein is accurate at the date of submission. It is important to request that individuals inform us if their information changes, and this reminder should be sent at regular intervals.

Employees/Staff/Pupil's Guardians/Suppliers must notify L.E.A.D. Academy Trust of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are located on the L.E.A.D. Academy Trust portal Any notification regarding change of circumstances must be promptly recorded and acted upon.

Employees/Staff of L.E.A.D. Academy Trust are responsible for ensuring that any Personal Data about them and supplied by them to L.E.A.D. Academy Trust is accurate and up-to-date.

The DPO/ GDPR Owner is responsible for ensuring that appropriate procedures and policies are in place to keep Personal Data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors. On at least an annual basis, the DPO/ GDPR Owner will review the retention dates of all the Personal Data processed by L.E.A.D. Academy Trust, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure (GDPR-C DOC 11.2.7).

Any requests received by individuals to rectify their Personal should be sent to the DPO/ GDPR Owner, who is responsible for responding to requests for rectification from Data Subjects within one month (Subject Access Request Procedure GDPR DOC 2.2). This can be extended to a further two months for complex requests. If L.E.A.D.

Academy Trust is unable to comply with the request, the DPO/ GDPR Owner must respond to the Data Subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

Where third-party organisations have been passed inaccurate or out of date information, the DPO/GDPR Owner is responsible for making appropriate arrangements to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the Personal Data to the third party where this is required.

5.6 **Data Minimisation**

It is important to ensure that we limit the Personal Data that L.E.A.D Academy Trust holds to the extent that it is absolutely necessary in relation to the purpose for which it is used. Where Personal Data is retained beyond the Processing date, it will be encrypted in order to protect the identity of the Data Subject in the event of a data breach. The processing date refers to the date of which data is required to be used within the trust/school to deliver education. After which other than legally required data, the data is removed from the systems.

L.E.A.D Academy Trust has in place a Retention of Records Procedure (GDPR DOC 2.3), which explains how long certain Personal Data records should be kept for. Once the 'retention period' for a piece of Personal Data has passed, the data must be securely and permanently destroyed as set out in this procedure. This is vital to ensure all Personal Data is held lawfully and in accordance with its purpose. The Retention of Records Procedure can be found at the Academy Trust portal.

If Personal Data is being retained beyond the specified retention period contained within the Retention of Records Procedure, it must be expressly approved by the DPO/. The justification for retaining the data beyond the retention period must be clearly identified and in line with the requirements of the data protection legislation. Approval by the DPO/GDPR Owner must be given in written format. If you identify any **Personal** Data that is being retained beyond its retention period, you must inform the DPO/GDPR Owner without delay.

5.7 **Personal Data must be processed in a manner that ensures the appropriate security**

Ensuring the upmost security over the Personal Data held by the Trust is pivotal to protecting the Personal Data from data breaches. It is important to L.E.A.D Academy Trust that sufficient technical measures are put in place to ensure the safety and protection over the Personal that is processed by the organisation.

Examples of technical measures that may be considered appropriate by the DPO/ GDPR Owner include:

- Password protection (GDPR-C DOC 9.2.3);
- Automatic locking of devices that are not being actively used;

- Removal of access rights for removable storage devices (GDPR-C DOC 9.1.2 & GDPR DOC 11.2.7);
- Virus checking software and firewalls (GDPR-C DOC 6.2.1);
- Role-based access rights including those assigned to temporary staff (GDPR-C DOC 9.1.2);
- Encryption of devices that leave the organisations premises such as laptops and mobile phones (GDPR-C DOC 6.2.1);
- Security of local and wide area networks (GDPR-C DOC 6.2.1);
- Privacy enhancing technologies such as pseudonymisation and anonymisation; and
- Identifying appropriate international security standards relevant to L.E.A.D. Academy Trust.

In addition to technical security measures, organisational measures may also be implemented to assist in ensuring security and safety of the Personal processed by the Trust. When determining what measures should be put in place, the DPO/ GDPR Owner will consider the following:

- The appropriate training levels throughout L.E.A.D. Academy Trust;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of Personal Data and storing the media off-site; and
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the UK.

These controls have been selected on the basis of identified risks to Personal Data, and the potential for damage or distress to individuals whose data is being processed.

5.8 **The Trust must be able to demonstrate compliance with the UK GDPR's other principles (accountability)**

The UK GDPR includes provisions that promote accountability and governance. These complement the UK GDPR's transparency requirements. The accountability principle in Article 5(2) requires L.E.A.D. Academy Trust to demonstrate that the Trust complies with the principles and states explicitly that this is the responsibility of the Trust.

The L.E.A.D. Academy Trust will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

The Trust is committed to continuously improving its data privacy compliance, and will continue to document its compliance, progress and developments to policies and procedures to demonstrate this ongoing improvement.

The Trust will maintain records of all AI systems processing personal data, including the purposes, categories of data, and logic of processing.

The Data Protection Officer will oversee compliance with GDPR in relation to AI and ensure that staff are trained on the risks and responsibilities associated with AI.

6. Data Subjects' rights

Data Subjects have a number of rights in relation to the Processing of their Personal Data, including:

- Right to access - Individuals have a right to make a subject access request. If an individual makes a subject access request, L.E.A.D Academy Trust will follow the Subject Access Request Procedure (GDPR DOC 2.2); this procedure describes how an individual can make a subject access request, and how L.E.A.D. Academy Trust will ensure that its response to the data access request complies with UK GDPR. A link to this procedure can be found here in the Academy Trust portal].

- Right to be informed – individuals have the right to be informed about the collection and use of their Personal Data and to obtain details of the purposes of Processing, the retention periods, and who it is shared with.

- Right to object – individuals can object to the Processing of their Personal Data in certain circumstances. For example, individuals have an absolute right to prevent Processing for purposes of direct marketing, and this includes any Profiling of data related to direct marketing. If the Trust is Processing the Personal Data relying on legitimate interests or upon fulfilling a public task, the individual can give specific reasons for objecting to the Processing such as it causing them substantial damage or distress.

- Right to be informed about the mechanics of any automated decision-making processes and Profiling that will significantly affect them.

- Right to not be subject to a decision based solely on automatic Processing, including Profiling, which has a significant impact on them.

- Right to rectification – individuals have a right for inaccurate Personal Data to be rectified, or completed if it is incomplete.

- Right to be forgotten – individuals have a right for their Personal Data to be erased. This is not an absolute right and only applies in certain circumstances.

- Right to portability - to have Personal Data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another Controller.

- Right to complain – an individual has a right to complain to the UK's supervisory authority, the Information Commissioner's Office, if they believe that a provision of the UK GDPR has been contravened. In addition, Data Subjects have the right to complain to L.E.A.D. Academy Trust related to the Processing of their Personal Data, the handling of a request from a Data Subject and appeals from a Data Subject on how complaints have been handled in line with the Complaints Procedure (GDPR DOC 2.9). A link to our Complaints Procedure can be found at our trust website www.leadacademytrust.co.uk.

- Under data protection law, individuals have a right to take their case to court to enforce their rights if they believe they have been breached, and to claim compensation for any damage caused by any organisation in contravention of the UK GDPR.

- Data Subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significant impacts.

- Where such processing is necessary, the Trust will provide meaningful information about the logic involved, as well as the significance and envisaged consequences for the Data Subject.

- Data Subjects may request human intervention, express their point of view, and contest the decision.

7. Security of data

7.1 All Employees/Staff are responsible for ensuring that any Personal Data that L.E.A.D. Academy Trust holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by L.E.A.D. Academy Trust to receive that information and has entered into a confidentiality agreement.

7.2 All Personal Data should be accessible only to those who need to use it as part of their role within L.E.A.D. Academy trust, and access may only be granted in line with the

Access Control Policy (GDPR-C DOC 9.1.1). All Personal Data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy (GDPR-C DOC 9.1.1); and/or
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media (GDPR-C DOC 11.2.7).

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of L.E.A.D. Academy Trust. All Employees/Staff are required to enter into an Acceptable Use Agreement (GDPR-C DOC 9.2.1A) before they are given access to organisational information of any sort.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit, documented, [written] authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the data retention policy.

7.5 Personal Data may only be deleted or disposed of in line with the Retention of Records Procedure (GDPR DOC 2.3). Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by GDPR-C DOC 11.2.7 before disposal.

7.6 Processing of Personal Data 'off-site' presents a potentially greater risk of loss, theft or damage to Personal Data. Staff must be specifically authorised to process data off-site.

7.7 The Trust will implement appropriate technical and organisational measures to ensure the security of personal data processed by AI systems, including regular audits and monitoring for bias, fairness, and accuracy.

7.8 AI systems will be included in the Trust's data inventory and subject to regular review as part of the PIMS.

8. Disclosure of data

8.1 L.E.A.D. Academy Trust is required to ensure that Personal Data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose Personal Data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of L.E.A.D. Academy

Trust's business.

8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO / GDPR Owner.

9. Retention and disposal of data

9.1 L.E.A.D. Academy Trust shall not keep Personal Data in a form that permits identification of Data Subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 L.E.A.D. Academy Trust may store data for longer periods if the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the Data Subject.

9.3 The retention period for each category of Personal Data will be set out in the Retention of Records Procedure (GDPR DOC 2.3) along with the criteria used to determine this period including any statutory obligations L.E.A.D. Academy Trust has to retain the data.

9.4 L.E.A.D. Academy Trust's data retention and data disposal procedures (Storage Removal Procedure GDPR-C DOC 11.2.7) will apply in all cases.

9.5 Personal Data must be disposed of securely in accordance with the sixth principle of the UK GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of Data Subjects. Any disposal of data will be done in accordance with the secure disposal procedure (GDPR-C DOC 11.2.7).

10. Personal Data Breaches

10.1 A Personal Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. It covers malicious incidents such as cyber-attacks, and incidents arising as a result of human error, for example a lost laptop, device or file, or sending personal details to an incorrect email address.

10.2 If L.E.A.D Academy Trust discovers there has been a Personal Data Breach that poses a risk to the rights and freedoms of individuals, it may need to report it to the Information Commissioner's Office within 72 hours of discovery. It is therefore vital that if you suspect there has been a security breach, you must inform the DPO/GDPR Owner immediately as we are required to report data breaches within very strict timescales.

11. Transferring Personal Data to third parties

11.1 Third parties such as companies, businesses, suppliers or customers outside of L.E.A.D Academy Trust may, from time to time, need access to the Personal Data we process, for example as part of providing services to us. However, we are only permitted to disclose Personal Data to third parties in limited circumstances.

11.2 When the Trust is transferring Personal Data with countries outside of the United Kingdom, additional levels of protection are required. L.E.A.D Academy Trust will ensure that the correct mechanisms are put into place to ensure privacy considerations are addressed, and this generally means that additional clauses must be included in the contract.

11.3 When deciding whether to transfer data to a third party, L.E.A.D Academy Trust will conduct due diligence and ensure that the third party provides sufficient guarantees with respect to data security and handling Personal Data generally. The Trust will consider a number of factors including: the nature of the information being transferred; the country or territory of origin and the final destination of the information; how the information will be used for and how long; the laws and practices of the country of the transferee; and the security measures that are to be taken in the overseas location.

11.4 In the absence of appropriate legal safeguards (for example a UK adequacy decision, UK-US data bridge membership, additional contractual clauses), a transfer of Personal Data to a third country or international organisation shall only take place on one of the following conditions:

- the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;

- the transfer is necessary for the performance of a contract, or the implementation of pre-contractual measures taken at the Data Subject's request;

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;

- the transfer is necessary for important reasons of public interest;

- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

11.5 You should always check with the DPO/GDPR Owner if you are unsure whether or not you are permitted to disclose Personal Data to a third party.

12. Information asset register/data inventory

12.1 L.E.A.D. Academy Trust has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. L.E.A.D. Academy Trust's data inventory and data flow determines (GDPR DOC 2.4, and GDPR REC 4.4):

- business processes that use Personal Data;
- source of Personal Data;
- volume of Data Subjects;
- description of each item of Personal Data;
- Processing activity;
- maintains the inventory of data categories of Personal Data processed;
- documents the purpose(s) for which each category of Personal Data is used;
- recipients, and potential recipients, of the Personal Data;
- the role of the L.E.A.D. Academy Trust throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

12.2 L.E.A.D. Academy Trust carries out an assessment of risks associated with the Processing of particular types of Personal Data.

12.3 L.E.A.D. Academy Trust assesses the level of risk to individuals associated with the Processing of their Personal Data. When taking into account the scope, context and purpose of Processing, it is deemed that is likely to result in a high risk to the rights and freedoms of individuals, a data protection impact assessments (DPIA) must be undertaken by the Trust **prior** to the Processing taking place (DPIA Procedure GDPR DOC 2.4 and GDPR REC 4.4).

12.4 The DPIA risk assessment covers Processing undertaken by L.E.A.D Academy Trust, and by other organisations on behalf of L.E.A.D. Academy Trust. When undertaking a risk assessment, L.E.A.D. Academy Trust will consider the risks of undertaking the Processing in proportionality to the purposes, the threat on individual's rights and freedoms and the possible impact. The extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on L.E.A.D. Academy Trust itself, and any likely reputational damage including the possible loss of customer trust will also be considered. A single DPIA may address a set of similar Processing operations that present similar high risks.

12.5 Where, as a result of a DPIA, it is clear that L.E.A.D. Academy Trust is about to commence Processing of Personal Data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not L.E.A.D. Academy Trust may proceed must be escalated for review to the DPO/GDPR Owner.

12.6 The DPO/ GDPR Owner shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

12.7 Appropriate controls will be selected, as detailed in Annex A of ISO 27001, ISO 27017, ISO 27018 and applied to reduce the level of risk associated with Processing individual data to an acceptable level, by reference to L.E.A.D. Academy Trust's documented risk acceptance criteria and the requirements of the UK GDPR.

12.8 If you are considering Processing data in a new or novel way, or wish to implement a new product or process that uses, transmits or stores Personal Data, it is important to consider if a DPIA is required. Please contact the DPO/GDPR Owner to discuss this further.

13. Document Owner and Approval

The DPO / GDPR Owner is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on L.E.A.D. Academy Trust Site.

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Lee Jepson	16/04/2018
2	Reviewed with slight amendments	Lee Jepson	09/07/2020
3	Reviewed minor amendments	Lee Jepson	29/06/2021
4	Reviewed minor amendments for GDPR and CCTV	Lee Jepson	05/10/2022
5	Reviewed and updated	Lee Jepson	31/08/2023
6	Reviewed and updates	Lee Jepson	31/08/2024
7	Reviews and checked by Eversheds	Lee Jepson	31/08/2025
8	AI Additions	Lee Jepson	1st December 2025