Records Management Policy

Document Control

Version	Author	Summary of Changes	Approved By	Date Published	Date of Review
1	RGR	New	Trust Board	Feb 2020	Mar 2021
2	RGR	New template; change GDPR to UK-GDPR; update to 1.3	Trust Board	Mar 2021	Mar 2022
3	RGR	Annual Review	Trust Board	Mar 2022	Mar 23
4	RGR	Annual Review	Trust Board	Mar 2023	Mar 2024
5	RGR	Update 1.2; 5.2; 8.2	Trust Board	Mar 2024	Mar 2025
6	RGR	Update 6.2 to add electronic visitor management systems; IRMS	CEO	Mar 2025	Mar 2028

Contents

STATEMENT OF INTENT

Leger Education Trust is committed to maintaining the confidentiality of its data and ensuring that all records within the Trust and its Academies are only accessible by the appropriate individuals. In line with the requirements of UK-GDPR, the Trust's Academies also have a responsibility to ensure that all records are only kept for as long as it necessary to fulfil the purpose(s) for which they were intended.

The Trust has created this policy to outline how records are stored, accessed, monitored, retained and disposed of in order to meet Leger Education Trust's statutory requirements.

1. LEGAL FRAMEWORK

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

- UK-GDPR
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)

1.2 This policy also has due regard to the following guidance:

- DfE (2018) 'Data Protection: A Toolkit for Schools'
- IRMS Toolkit for Schools (2024)

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

- Data Protection Policy
- Freedom of Information Policy
- Disposal of Records Log
- Data Asset Register
- Bring Your Own Device and Acceptable Use Policy

2. RESPONSIBILITIES

2.1 Each Academy has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

2.2 Each Principal holds overall responsibility for the policy and for ensuring it is implemented correctly.

2.3 The Data Protection Officer (DPO) is responsible for the management of records for the Trust/its Academies.

2.4 The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with each Principal.

2.5 The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of correctly.

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

3. MANAGEMENT OF STUDENT RECORDS

3.1 Student records are specific documents that are used throughout a student's time in the education system – they are passed to each School/Academy that a student attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.

3.2 An electronic student management system (e.g. SIMS) is used to store other student data and is accessible to staff; data stored includes:

- Ethnic origin, religion and first language (if not English)

- Any preferred names
- Siblings in the Academy
- Emergency contact details
- Any allergies or other medical conditions that are important to be aware of
- Names of parents/carers, including their home address(es) and telephone number(s)
- Name of the Academy, admission number, the date of admission and the date of leaving, where appropriate
- Any other agency involvement, eg speech and language therapist

3.3 The following information is also stored on SIMs and will be easily accessible to staff:

- Admissions form (paper copies kept with data office)
- Details of any SEND
- If the student has attended a primary/other secondary school, the record of transfer
- Assessment Point reports to parents/carers
- Notes relating to major incidents and accidents involving the student
- Any information about an education, health and care (EHC) plan and support offered in relation to the EHC plan
- Any information relating to exclusions
- Any correspondence with parents/carers or external agencies relating to major issues
- Notes indicating that records of complaints made by parents/carers or the student are held

3.4 The following information is subject to shorter retention periods and therefore, will be stored separately:

- Absence notes
- Parental and, where appropriate, student consent forms for educational visits, photographs and videos, etc.

3.5 For security purposes safeguarding information including disclosures and reports relating to child protection are stored on CPOMs which has restricted access; if any paper copies are held then they are kept in a securely locked filing cabinet.

3.6 Hard copies of complaints made by parents/carers or students are stored in a file centrally – a note indicating this is marked on the student's file.

3.7 Actual copies of accident and incident information are stored separately on the Academy's secure file server which has restricted access and held in line with the retention periods outlined in this policy. An additional copy may be placed in the student's file in the event of a major accident or incident.

3.8 The Academy will ensure that no student records are altered or amended before transferring them to the next School/Academy that the student will attend. (NB records will be anonymised to remove other student names and also staff names as appropriate)

3.9 The only exception to the above is if any records placed on the student's file have a shorter retention period and may need to be removed. In such cases, the DPO responsible for disposing records, will remove these records.

3.10 Electronic records relating to a student's record will also be transferred to the student's next School/Academy. Section 11 of this policy outlines how electronic records will be transferred.

3.11 If any student attends the Academy until statutory school leaving age, the Academy will keep the student's records until the student reaches the age of 25 years.

3.12 The Academy will, wherever possible, avoid sending a student record by post. Where a student record must be sent by post, it will be sent by registered post with an accompany list of the files included. The

School/Academy it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the relevant Leger Education Trust Academy.

4. IRMS

4.1 The retention periods for documentation is as per the IRMS Toolkit IRMS Schools Toolkit - Information and Records Management Society

This can be found here: LET Records Management Policy IRMS_2024.pdf

5. IDENTIFYING INFORMATION

5.1 Under the UK-GDPR, all individuals have the right to data minimisation and data protection by design and default – as the Data Controller, the Academy ensures appropriate measures are in place in order for individuals to exercise this right.

5.2 Wherever possible, the Academy uses pseudonymisation, also known as the 'blurring technique' to reduce risk of identification.

5.3 Once an individual has left the Academy, if identifiers such as names and dates of birth are no longer required, these are removed or less specific personal data is used, e.g. the month of birth rather than specific date – the data is blurred slightly.

5.4 Where data is required to be retained over time, e.g. attendance data, the Academy removes any personal data not required and keeps only the data needed – in this example, the statistics of attendance rather than personal information.

6. STORING AND PROTECTING INFORMATION

6.1 The DPO will undertake a risk analysis to identify which records are vital to Academy management and these records will be stored in the most secure manner.

6.2 See IT Security Policy for details about how data is backed-up.

6.3 Where possible, backed-up information will be stored off the Academy premises.

6.4 Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.

6.5 Confidential paper records are not left unattended or in clear view when held in a location with general access.

6.6 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site.

6.7 USBs/portable hard drives are not used to hold personal information unless they are password-protected and fully encrypted and staff have specific permission from the CEO to have such a device.

6.8 All electronic devices are password-protected to protect the information on the device in case of theft.

6.9 Where possible, the Academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

6.10 When working off-site, staff should log in via the virtual desktop/Academy Office 365 account to ensure no student/staffs' personal data is held on personal computers/laptops/tablets etc.

6.11 All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

6.12 Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.

6.13 Circular emails to parents/carers are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. This should also be the case for circular emails to a variety of organisations where recipients do not know each other/have not shared email contacts.

6.14 When sending confidential information by fax, members of staff always check that the recipient is correct before sending.

6.15 Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the UK-GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from Academy premises accepts full responsibility for the security of the data.

6.16 Before sharing data staff always ensure that:

- They have consent from data subjects to share it
- Adequate security is in place to protect it
- The data recipient has been outlined in a privacy notice.

6.17 All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet drawer or safe with restricted access.

6.18 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Academy containing sensitive information are supervised at all times.

6.19 The physical security of Trust buildings and storage systems, and access to them, is reviewed termly by the site manager in conjunction with the DPO.

6.20 The Trust takes its duties under the UK-GDPR seriously and any unauthorised disclosure may result in disciplinary action.

6.21 The DPO is responsible for continuity and making sure recovery measures are in place to ensure the security of protected data.

6.22 Any damage to, or theft of, data will be managed in accordance with the Trust's Security Breach Management Plan.

7. ASSESSING INFORMATION

7.1 All Trust Academies are transparent with data subjects, the information held and how it can be processed.

7.2 All members of staff, parents/carers of registered students and other users of each Academy, eg visitors and third party clubs, are entitled to:

- Know what information the Academy holds and processes about them or their child and why

- Understand how to gain access to it

- Understand how to provide and withdraw consent to information being held

- Understand what the Academy is doing to comply with its obligations under the UK-GDPR.

7.3 All members of staff, parents/carers of registered students and other users of the Academy and its facilities have the right, under the UK-GDPR, to access certain personal data being held about them or their child.

7.4 Personal information can be shared with students once they are considered to be at an appropriate age and responsible for their own affairs; although this information can still be shared with parents/carers.

7.5 Students who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

7.6 Each Academy will adhere to the provisions outlined in the Trust's Data Protection Policy when responding to requests seeking access to personal information.

8. DIGITAL CONTINUITY STATEMENT

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

8.2 The DPO will identify any digital data that will need to be named as part of a digital continuity statement.

8.3 The data will be archived to dedicated files on the Academy's server, which are password-protected – this will be backed-up in accordance with Section 11 of this policy.

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

8.5 The IT department will review new and existing storage methods annually and, where appropriate, add them to the digital continuity statement.

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

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

9. INFORMATION AUDIT

9.1 The Trust conducts information audits on an annual basis against all information held by each Academy to evaluate the information each Academy is holding, receiving and using, and to ensure that this is correctly managed in accordance with the UK-GDPR. This includes the following information:

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

9.2 The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows etc.
- Questionnaires to key staff members to identify information and information flows etc.

- A mixture of the above.

9.3 The DPO is responsible for completing the information audit. The information audit will include the following:

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

9.4 The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.

9.5 Once it has been confirmed that the information is accurate, the DPO will record all details on the Academy's Data Register.

9.6 The information displayed on the Data Register will be shared with each Principal to gain their approval.

10. Disposal of Data

10.1 Where disposal of information is outlined as standard disposal, this will be re-cycled appropriate to the form of the information, e.g. paper re-cycling, electronic re-cycling.

10.2 Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut. The DPO will keep a record of all files that have been destroyed.

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

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

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

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