Data Protection Policy

This policy applies to the Lighthouse Learning Trust and all of its institutions. For the sake of brevity, references to the "Trust" in the policy document are taken to mean both the Trust itself as well as all of its individual institutions.

Publication Date	13 May 2021
Version Number	1.3
Related Legislation & Guidance	General Data Protection Regulation (GDPR) Data Protection Act 2018 Protection of Freedoms Act 2012 Information Commissioner's Office Guidance
Related Policies, Strategies and Other Documents	Data Retention Policy Information Security Policy CCTV Policy Safeguarding and Child Protection Policy Freedom of Information Publication Scheme
Replaces	No previous policy
Policy Owner	Data Protection Policy
Approval Level	Trust Board
Policy Author	Clerk to the Trustees and Company Secretary
Applies To	All employees, volunteers, and contractors of Lighthouse Learning Trust, including trainees and agency workers
Date Communicated to Staff	TBC
Responsibility for Deployment	Chief Executive, Trust Executive Team and Heads of College
Last Review	May 2021
Meeting Date/Minute Reference	13/05/2021
Next Review Due	July 2022 or as needed

This Policy Is informed by the Founding Principles of the Trust

Teaching and Learning – the pursuit of high quality teaching is the first priority of the trust. By ensuring high standards and achievement, and excellent progress and progression, it will improve the lives and life chances of our students.

Value for money – the trust must bring benefit to students. Management structures and shared support services must be efficient and effective, ensuring that resources for teaching and learning are maximized.

Inclusivity – member organisations are committed to the full range of students in their communities. They adopt a 'growth mind-set' attitude and seek improved outcomes through the quality of provision and curriculum and not through selection or exclusion.

Safety – The trust will provide students and staff with a safe environment based on respect for all and free from prejudice and intimidation.

Accountability – we are accountable to our communities who fund our activity and, rightly, expect excellence and professionalism in all that we do.

Integrity – member institutions and their staff are on a journey of self-improvement. This requires honesty, a self-critical culture, evidence-based analysis and a rejection of arrogance.

Celebration – helping people progress through education is a privilege. We celebrate our successes, our students' successes and those of our partner institutions.

1. What is the Purpose of this Policy?

1.1 The Lighthouse Learning Trust ("the Trust") needs to collect certain types of personal information about the people with whom it deals, including its current and past students, their parents, and employees of the Trust. This information has to be collected for administrative purposes, but also to support the teaching, learning, and safeguarding of students. In some cases, it is needed to fulfil legal obligations to the Education and Skills Funding Agency, the Department for Education, local authorities, and other government bodies.

1.2 The Lighthouse Learning Trust is committed to compliance with the General Data Protection Regulation (GDPR) and with the Data Protection Act 2018. The Trust will also seek to comply with guidance provided by the Information Commissioner's Office (ICO).

1.2 The Trust is a "Data Controller" as defined by the GDPR. This means that the Trust must protect the rights and freedoms of people when processing their personal data. The purpose of this policy document is to explain how the Trust will do this.

2. What is Personal Data?

2.1 Personal data is information that relates to an identified or identifiable living individual.

What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.

If it is possible to identify an individual directly from information that is being processed, then that information is likely to be personal data.

Some personal data requires more protection because it is sensitive – this is known as "special category data"

The GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;

• **biometric data** (where used for identification purposes);
• data concerning **health**;
• data concerning a person's **sex life**; and
• data concerning a person's **sexual orientation**.

3. Who is this Policy For?

3.1 This policy should be applied by all employees of the Trust as well as any volunteers, secondees, and contractors. Compliance with this policy is mandatory, and breaches may be considered to be a disciplinary matter.

3.2 This policy applies to all personal data processing functions within the Trust as well as to any other personal data processed by the Trust from any other source regardless of its format

3.3 Third parties who work with or have a relationship with the Trust will be expected to comply with this policy and with the GDPR and UK Data Protection legislation.

4. Roles and Responsibilities

4.1 All of the Trust's employees have a personal responsibility to ensure that personal data that they come in contact with is processed safely and appropriately, and in compliance with this policy.

4.2 The Trust's executive team and the senior leadership teams at each college will ensure that all those in managerial or supervisory roles are responsible for developing and encouraging good data protection practices within their own areas of responsibility.

4.3 A Data Protection Officer (DPO) (a role specified within the GDPR) will be appointed by the Board and will report to the Trust Chair and Chief Executive. This role will be performed by an individual who is independent of the Trust's data processing functions. The responsibilities of the DPO are:

(a) To inform and advise the Trust and its employees about their GDPR obligations and compliance with data protection legislation, including through training.
(b) To monitor levels of compliance with GDPR across the Trust.
(c) To draft the Trust's Data Protection Policy and ensure that this is regularly reviewed

(d) To review GDPR-related documentation across the Trust and ensure that this reflects best practice
(e) To review and sign-off Data Privacy Impact Assessments (DPIAs)
(f) To manage, record, and report personal data breaches.
(g) To manage, record, and report compliance with Subject Access Requests.
(h) To present an annual GDPR report to the Trust Board

4.4 The Director of MIS, Funding & Systems will also play a key role in ensuring Trust-wide compliance with GDPR. This postholder will:

(a) Maintain the Trusts' Information Asset Register.
(b) Maintain a data flow process map of the Trust's data systems showing clearly where and how data is held, classified, and processed.
(c) Implement appropriate technical and organisational measures to show that the Trust has considered and integrated the principles of data protection into its processing activities.
(d) Draft the Trust's Data Retention Policy and ensure that this is regularly reviewed.
(e) Develop and deploy Information Security Policies in collaboration with the IT Manager.
(f) Oversee the completion of Data Privacy Impact Assessments (DPIAs) as required by GDPR
(g) Oversee the compliance of third-party contracts for data processing, and conduct due diligence.

4.5 The Trust will ensure that the roles described in paras. 3.3 and 3.4 above are properly and specifically resourced.

5. Data Protection Principles

5.1 Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime. The Trust is committed to compliance with these principles.

Article 5(1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals **('lawfulness, fairness and transparency'**);

(b) 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 to be incompatible with the initial purposes **('purpose limitation'**);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);

(d) 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 **('accuracy'**);

(e) 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 GDPR in order to safeguard the rights and freedoms of individuals ('**storage limitation'**);

(f) 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 ('**integrity and confidentiality'**)."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability'**)."

6. Information Asset Register/Data Inventory

6.1 The Lighthouse Learning Trust will maintain a data inventory and data flow process map as a means of identifying and mitigating GDPR related risks. This inventory and data map will be maintained by the Director of MIS, Funding & Systems. Any risks identified in this way will be addressed by the Trust's risk management processes.

7. Data Protection Impact Assessments (DPIAs)

7.1 The Director of MIS, Funding & Systems will oversee the completion of Data Protection Impact Assessments (DPIA) as required by the GDPR. In particular DPIA's will be conducted where new or changing technologies are being deployed; where automated processing is taking place; where large scale processing of special category data is required; and with regard to large scale systematic monitoring of a publicly accessible area (e.g. through the use of CCTV).

7.2 DPIAs will contain a description of the proposed processing and its purposes; an assessment of its necessity and proportionality; an assessment of the risk to individuals; and a statement regarding any risk mitigation measures that have been put in place.

8. Data Accuracy – Students and Employees

8.1 All students and employees must make sure that any personal data they provide to the Trust is accurate and up to date. They should inform the Trust if any of their personal data changes, or if they become aware that any of the information held by the Trust about them is not accurate.

9. Security of Data

9.1 All employees are responsible for ensuring that any personal data held by the Trust is kept securely and is not under any circumstances disclosed to external third parties unless that third party has been specifically authorised by the Trust to receive such information. Where there is a need to share data with a third party, the Trust will carry out due diligence and take reasonable steps to ensure that data will be stored securely and adequately protected.

9.2 All personal data should be accessible only to those who need to use it for a function of the Trust or its colleges.

9.3 All personal data should be treated with the highest security in mind. In particular, the following steps should routinely be taken to protect personal data:

(a) Electronic documents containing personal data must be password protected. Document passwords should be communicated to the recipient in a separate communication from that which contains the document (e.g. a separate email).

(b) Hard copy documents must be kept in locked drawers or cabinets and not removed from Trust premises without authorisation from a line manager (in which case documents should be signed for both in and out of Trust premises, and a log maintained).

(c) Computer screens and terminals displaying personal data should not be visible to anyone other than authorised staff. Manual records must not be left unattended at any time.

(d) Personal data should not generally be stored on personal or portable devices such as memory sticks, laptops etc. Where this is unavoidable, encryption software should be used to protect these devices.

(e) The blind copy function must always be used when sending group emails to recipients outside of the organisation.

(f) Processing data whilst working remotely at home presents a potentially greater risk of loss. Line managers should therefore be particularly vigilant in reminding staff who are working remotely of their GDPR responsibilities and conduct risk-assessments where there are any particular concerns.

10. Photography and Filming Consent

10.1 The Trust will seek written consent from students before publishing their images (for any purpose) as captured in photographs, video recordings, or in any other format.

11. Video-Conferencing

11.1 When using any video-conferencing application (e.g. Zoom) meetings must not be recorded unless:

-a lawful basis for processing the data content has been established

-a data protection impact assessment (DPIA) has been created and signed off by the DPO

-consent to the recording is given verbally by all of those present before the recording is made

12. Biometric Recognition Systems

12.1 Where the Trust uses a student's biometric data as part of an automated biometric recognition system it will comply with the requirements of the Protection of Freedoms Act 2012. The Trust will seek written consent before any biometric data is collected or processed. A student has the right not to participate in the processing of biometric data, and may withdraw their consent at any time if it has been previously given.

12.2 Where employees or other adults are asked to use a biometric system by the Trust, written consent will also be sought in advance. As with students, employees of the Trust or other adults have a right not to participate in the processing of biometric data, and may withdraw their consent at any time if it has been previously given.

13. Breaches of Personal Data

13.1 All personal data breaches must be reported to the Data Protection Officer without delay. Once a breach is known about, the Data Protection Officer should be made aware on the same working day or, at the latest, with 24 hours.

13.2 The Data Protection Officer will investigate the breach, assess the risk to those affected by it, and decide whether or not the breach should be reported to the Information Commissioner's Office (ICO). The breach will also be reported to those

who may potentially be affected or placed at risk by the breach. All reports to the ICO will be made within 72 hours of the breach being notified to the Data Protection Officer. The Data Protection Officer will maintain a log of all breaches and record the actions taken by the Trust in response to these. All breaches will be reported to the Trust Board annually, or earlier if Trust-wide action is required.

14. Data Subjects' Rights

14.1 Individuals have a right to make a 'subject access request' (SAR) in order to gain access to personal information held about them by the Trust and/or its colleges. Such requests may be received at any point in the organisational structure and can be made either verbally or in writing.

14.2 Individuals are entitled:

- To be informed whether your personal data is being processed by the Trust
- To be sent a copy of your personal data (subject to any applicable exemptions)
- To be sent certain information about your personal data

All subject access requests must be reported by the recipient to the Data Protection Officer so that a response can be planned in line with statutory requirements. In all cases the Trust will respond to a subject access request within one month from the day of receipt. In most circumstances, the Trust will not charge a fee for dealing with such requests.

14.3 Students have a right of access to their own information. When a student cannot act for themselves or the student gives permission, parents will be able to access this information on their behalf. In academies there is no automatic or independent parental right of access to a child's educational record, although any such requests can be considered by college leaders on a case- by- case basis.

14.4 If, on receipt of the Trust's response to your request you consider that the Trust has not dealt correctly with your request, then please contact the Data Protection Officer. If you are still not satisfied, your should contact the Information Commissioner's Office

15. Retention and Disposal of Data

15.1 The Trust will not keep personal data in a form that permits the identification of data subjects for any longer than is necessary. The retention period of each category of personal data will be specified in the Trust's Data Retention Policy. The disposal of data that is no longer required will be carried out securely.

16. GDPR Training

16.1 All employees, Trustees, and Local Governors will be provided with data protection training as part of their induction process.

16.2 Data protection training will also form part of continuing professional development where any changes to legislation, guidance, or the Trust's processes make it necessary.

16.3 All staff and volunteers will be expected to complete basic GDPR awareness training at least once every 3 years. This training will be delivered by means of an online module and will be compulsory. A more detailed and higher level awareness module will be completed by all staff with data handling responsibilities as well as by the CEO, the Trust Chair, MIS Director, HR Director, Finance Director, IT Manager, the Clerk to the Trustees, the Data Protection Officer, the Chair of the Governance and Audit Committee and Chairs of the Local Governing Bodies. Again, this training will be completed at least once in every 3 years. Training records will be maintained by the HR Team.

17. Contacts

17.1 The Data Protection Officer is Andrew McVittie.

Email: andrew.mcvittie@lighthouselearningtrust.ac.uk

17.2 The Director of MIS, Funding & Systems is Steve McDermott

Email: steve.mcdermott@lighthouselearningtrust.ac.uk