The Legacy Learning Trust

Data Protection Policy

Status & Review Cycle	Term	Year
Last Review Date/Policy Adopted	Autumn Term	2023-2024
Next Review Date	Autumn Term	2024-2025
Lead	DPO	

Contents **Page Number**

1. Policy Aims

1.1. The Legacy Learning Trust ('The Trust') collects and uses certain types of personal information about employees, students, parents and other individuals who come into contact with The Trust and its academies in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding.

1.2. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and other related legislation.

2. Statement of Intent

- The Trust will need to collect, store and process certain information about its employees, pupils and other service users, including personal and sensitive information.
- The Trust will be required to share personal information about its staff or pupils with other organisations, such as the Local Authority, DfE, educational bodies, and potentially children's services.
- This policy is in place to ensure that all staff and governors are aware of their responsibilities and outlines how The Trust complies with the principles of the UK GDPR.
- Organisational methods for keeping data secure are imperative, the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.
- This policy applies to all personal data held, irrespective of format (e.g. whether it is held on paper or on electronic media). The Trust is required to process personal data lawfully and therefore has taken the measures set out in this policy in order to comply with the UK GDPR.
- In order to carry out its statutory and administrative functions, The Trust needs to collect and process personal data relating to many categories of people, including students, employees, service users and suppliers.
- The Trust will only process personal data for such purposes and will disclose personal data to such third parties, as outlined in the appropriate privacy notice and in accordance with our Information Commissioner registration.
- Personal data will only be retained for as long as there is a genuine requirement to do so for a specified purpose, and will not be disclosed to any unauthorised third party (unless required by law or by statutory obligation).
- The aim is to provide a high standard of security for all personal data, whether it is stored electronically or in an alternative filing system. The level of security applied to sensitive personal data (as defined below) is regularly reviewed and monitored.
- This Policy does not form part of an employee's formal contract of employment but it is a condition of each employee's employment with The Trust or its Academies that the employee will abide by all rules and policies. Any failure by an employee to follow this Policy may, therefore, result in disciplinary action being taken.

3. Legal Framework

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

- The United Kingdom General Data Protection Regulation 2018
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The School Standards and Framework Act 1998.

3.2. This policy also has regard to the following guidance:

- ICO Guide to the General Data Protection Regulation (GDPR)
- DfE Data Protection: Toolkit for schools
- DfE Protection of biometric information of children in schools and colleges

3.3. This policy will be implemented in conjunction with the following other policies:

- Data Retention & Destruction Policy

4. Applicable Data & Definitions

4.1. The UK GDPR uses a number of technical terms which are defined here:

- **Data |** Information which is, or will be, processed automatically or manually within a relevant filing system. This includes but is not limited to written information, photographs and voice recordings. All manual data shall be deemed to be data for the purposes of this Policy.
- **Data Subject |** Any individual who is the subject of personal data.
- **Data Controller |** A person or organisation (e.g. The Trust or Academy) who determines the purposes for which and the manner in which personal data is, or will be, processed.
- **Data Processor |** A third party person or organisation (other than an employee of the Data Controller) who processes data on behalf of a Data Controller.
- **Personal Data |** Any Data relating to a living individual who can be identified from that Data or who is identifiable by combining the Data with other information available to the Data Controller (e.g. phone numbers and other contact information, photographs, video or audio recordings, National Insurance information etc); 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 |** Referred to in the UK GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 2018. These specifically include the processing of genetic data, biometric data and data concerning health matters. Personal data consisting of information regarding a Data Subject's racial or ethnic origin, political opinions, religious (or similar) beliefs, membership of a trade union, physical or mental health or condition, details of sexuality, commission or alleged commission of any offence and/or information relating to any proceedings and sentence for any committed or alleged offence of the Data Subject.
- **Biometric Data |** Defined under Article 4 of UK GDPR as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".
- **Processing |** Obtaining, recording or holding data, or carrying out any operation(s) on data, including organising, adapting, altering, retrieving, disclosing, erasure, destruction and combining with other information.
- **Processing biometric data |** Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it.

5. Principles

5.1. 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 to be 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 which is inaccurate, having regard to the purposes for which they are processed, is 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 principles".

6. Accountability

6.2. The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in-line with the principles set out in the UK GDPR.

6.3. The Trust will provide comprehensive, clear and transparent privacy policies. Additional internal records of The Trust'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.
- Clear desk and screen requirements (See Appendix 1)
- Description of technical and organisational security measures.
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

6.4. The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.
- Data protection impact assessments will be used, where appropriate.

7. Registration Agreement

7.1. The Legacy Learning Trust and its Academies are registered with the Information Commissioner's Office (ICO). The registration refers to the following:

7.2. Reasons/purposes for processing information:

- We process personal information to enable us to provide education, training, welfare and educational support services, to administer Trust property, maintain our own accounts and records, undertake fundraising; support and manage our employees. We also use CCTV for security and the prevention and detection of crime.

7.3. Type/classes of information processed:

We process information relevant to the above reasons/purposes. This may include:

- Personal details
- Family details
- Lifestyle and social circumstances
- Education and employment details
- Financial details
- Good and services
- Disciplinary and attendance records
- DBS Checks
- Visual images, personal appearance and behaviour

We also process sensitive classes of information that may include:

- Physical or mental health details
- Racial or ethnic origin
- Religious or other beliefs
- Trade union membership
- Sexual life
- Information about offences and alleged offences.

We process personal information about:

- Employees
- Pupils and their parents/carer/families
- Professional experts and advisers
- Board members, trustees and governors
- Directors
- Sponsors and supporters
- Suppliers and service providers
- Complainants and enquirers
- Customers
- Individuals captured by CCTV images.

7.4. We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the UK GDPR. What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons. Where necessary, or required, we share information with:

- Family, associates and representatives of the person whose data we are processing
- Educators and examining bodies
- Careers service
- Boards
- Local and central government
- Academy trusts
- Healthcare, social and welfare organisations
- Police forces and/or courts
- Current, past or prospective employers
- Voluntary and charitable organisations
- Business associates, professional advisers
- Suppliers and service providers
- Financial organisations
- Press and the media.

7.5. It may sometimes be necessary to transfer personal information overseas. Any transfers made will be in full compliance with all aspects of the UK GDPR. Where information must be shared beyond the UK, we ensure appropriate safeguards and assurances are taken that meet UK GDPR compliance standards and inform individuals through our privacy notices.

8. Data Protection Officer (DPO)

8.1. A Trust DPO has been appointed in order to:

- Inform and advise The Trust and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor The Trusts compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

8.2. An existing employee can be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests (when the DPO performs tasks that influence the way their employer uses personal data and make autonomous decisions about data processing activities).

As part of this role:

- The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to the education sector.
- The DPO will report to the highest level of management. (CEO, CFOO, Trustees)
- The DPO will not be dismissed or penalised for performing their task.
- Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR obligations.

9. Lawful Processing

9.1. 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:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- 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.

9.2. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by UK law.
- 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 on the basis of UK 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 on the basis of UK law or a contract with a health professional.
- 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 Article 89.

10. Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The school ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn, by the individual, at any time.
- Where a child is under the age of 13, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

11. Responsibilities of Employees

11.1. The most senior post holder within The Trust service or Academy are 'Information Asset Owners' and are responsible for ensuring that the requirements of UK GDPR are upheld and that steps are taken to ensure that all members of staff managing and processing personal data understand that they are responsible for following good data protection practice. A Data Protection Lead (DPL) should be identified within each School, or service function, to provide operational support.

11.2. In addition to the obligations set out elsewhere in this policy, all employees and volunteers are responsible for:

- Maintaining confidentiality and adhering to data protection legislation;
- Checking that any information that they provide to The Trust or Academy, in connection with their employment, is accurate and up to date.

- Informing The Trust or Academy of any changes to information which they have previously provided (e.g. change of address).
- Verifying the accuracy of any information previously provided to The Trust or Academy where required from time-to-time.
- Informing The Trust or Academy of any errors in the information held by The Trust or Academy about them. The Trust or Academy cannot be held responsible for any errors in an employee's information unless the relevant employee has informed The Trust or Academy of the error.
- All staff members should receive data protection training and be made aware of their responsibility to comply with data protection requirements.

11.3. If and when, as part of their responsibilities, employees collect information about other people (e.g. about colleagues, service users, pupils or details of personal circumstances), all employees must comply with the provisions of this Policy.

12. The Right to be Informed

12.1. All employees, pupils, service users and other individuals about whom The Trust or Academy processes personal data are entitled to:

- Know what information The Trust or Academy holds and processes about them and why.
- Be given a description of the recipients or classes of recipients to whom their personal data may be disclosed.
- Receive a copy of any information constituting their personal data held by The Trust or Academy (including information relating to the source of that data).
- Prevent the processing of their personal data for direct marketing purposes.
- Ask to have inaccurate personal data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

12.2. Employees should note that unauthorised disclosure of personal data by an employee will potentially lead to disciplinary action and may be considered gross misconduct in sufficiently serious or repeated cases.

12.3. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge. (See privacy notices).

12.4. If services are offered directly to a child, The Trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

12.5. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period or criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - ☐ Withdraw consent at any time
    - ☐ Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

12.6. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

12.7. Where data is not obtained directly from the data subject, information regarding the categories of personal data that The Trust holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

12.8. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

12.9. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

13. The Right to Access

13.1. Anybody whose personal data is processed by The Trust or its Academies (including but not limited to employees, pupils and service users) have the right (subject to certain statutory exemptions and restrictions) to access any personal data that is held about them (whether held on computer or manually).

13.2. Any person who wishes to exercise this right should submit the request in writing. Such requests should be immediately referred to the Data Protection Officer. The Trust aims to comply with requests for access to personal data as quickly as possible and will in any event provide a response within one calendar month (See Appendix 2).

13.3. Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

- The Trust or its Academies will verify the identity of the person making the request before any information is supplied. This may include a request for two separate forms of identification.
- A copy of the information will be supplied to the individual free of charge; however, The Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
    - All fees will be based on the administrative cost of providing the information.
- All requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- Where a request is manifestly unfounded or excessive, The Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.
- In the event that a large quantity of information is being processed about an individual, The Trust will ask the individual to specify the information the request is in relation to.

13.4. If an individual is not content with the information that has been disclosed in response to a SAR the individual will be entitled to request an internal review.

- The request for an internal review should be sent within 40 days and must clearly state the reference number and reason for the request for an internal review.
- The Trust will respond to a request for an internal review within 20 working days of receipt.

14. The Right to Rectification

- Individuals are entitled to have any inaccurate or incomplete personal data rectified.
- Where the personal data in question has been disclosed to third parties, The Trust will inform them of the rectification where possible.
- Where appropriate, The Trust or its Academies will inform the individual about the third parties that the data has been disclosed to.

- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- Where no action is being taken in response to a request for rectification, The Trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The Right to Erasure

15.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

15.2. Individuals have the right to erasure in the following circumstances:
Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

- When the individual withdraws their consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed.
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child.

15.3. The Trust and its Academies have the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.

15.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

15.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

15.6. Where personal data has been made public within an online environment, The Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

16. The Right to Restrict Processing

16.1. Individuals have the right to block or suppress The Trust's processing of personal data. In the event that processing is restricted, The Trust and its Academies will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

16.2. The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until The Trust has verified the accuracy of the data.
- Where an individual has objected to the processing and The Trust is considering whether their legitimate grounds override those of the individual.
- Where processing is unlawful and the individual opposes erasure and requests restriction instead.
- Where The Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.
- If the personal data in question has been disclosed to third parties, The Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- The Trust will inform individuals when a restriction on processing has been lifted.

17. The Right to Portability

17.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

17.2. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.
- When processing is carried out by automated means.

17.3. Personal data will be provided in a structured, commonly used and machine-readable form.

17.4. The Trust will provide the information free of charge.

17.5. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

17.6. In the event that the personal data concerns more than one individual, The Trust will consider whether providing the information would prejudice the rights of any other individual.

17.7. The Trust will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the time frame can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request. Where no action is being taken in response to a request, The Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

18. The Right to Object

18.1. The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

18.2. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest.
- Direct marketing.
- Processing for purposes of scientific or historical research and statistics.

18.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where The Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

18.4. Where personal data is processed for direct marketing purpose:

- The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes

18.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, The Trust is not required to comply with an objection to the processing of the data.

18.6. Where the processing activity is outlined above, but is carried out online, The Trust will offer a method for individuals to object online.

19. Automated decision-making and profiling

19.1. Individuals have the right not to be subject to a decision when:

19.2. It is based on automated processing, e.g. profiling.
It produces a legal effect or a similarly significant effect on the individual.

19.3. The Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it. When automatically processing personal data for profiling purposes, The Trust will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

19.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Trust has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of UK law.

20. Personal Data Breaches

20.1. A 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. This includes breaches that are the result of both accidental and deliberate causes. Personal data breaches can include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data.

20.2. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

20.3. The Trust DPO will determine whether the breach meets the respective thresholds for reporting to the ICO and notifying data subjects. The Trust must report the breach when, if not addressed in an appropriate and timely manner, it may result in:

- Physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights.
- Discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation.
- Damage to reputation.
- Loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

20.4. When reporting a breach, The Trust must provide:

- A description of the nature of the personal data breach.
- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of The Trust's DPO or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

20.5. If a breach is likely to result in a high risk to the rights and freedoms of individuals, The Trust must inform those concerned directly and without undue delay. Information provided to those affected must include:

- The name and contact details of The Trust's DPO or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, the measures taken to mitigate any possible adverse effects.

20.6. If the breach meets the thresholds for reporting, the DPO will do so within 72 hours of becoming aware of the breach. The DPO will be responsible for instigating an investigation into the breach, including how it occurred, and whether it could have been prevented. The Trust will review the outcome of the investigation, and review any recommendations for further training or changes in procedure and how they should be implemented. These recommendations will be reported to the Executive Team.

20.7. All breaches must be recorded internally.

21. Data Minimisation and Pseudonymisation

21.1. The Trust will implement appropriate technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

21.2. Where appropriate, The Trust will use pseudonymisation and other technical security measures to adhere to data-protection principles such as data minimisation and integrity and confidentiality, and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and DPA and protect the rights of data subjects.

22. Data Protection Impact Assessments (DPIA)

22.1. A DPIA enables the trust to systematically and comprehensively analyse its processing and to identify and minimise data protection risks. DPIAs take account of compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to

indicate that all risks have been eradicated, but it should help the trust to document them and assess whether any remaining risks are justified.

22.2. DPIAs are a legal requirement for processing that is likely to be high risk, but an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

22.3. The requirement for DPIAs is embedded in the trust's procurement process for new IT systems or software. The IT lead for each school will liaise with the trust's DPO regarding any planned procurement to ensure that the requirement for a DPIA is considered, and where appropriate a DPIA is carried out, before authorising any procurement request.

22.4. A DPIA must be made before the trust carries out any type of processing that is "likely to result in a high risk". This means that although the trust has not yet assessed the actual level of risk, it must screen for factors that point to the potential for a widespread or serious impact on individuals.

22.5. In particular, the GDPR says organisations must carry out a DPIA if a data controller plans to:

- Use systematic and extensive profiling with significant effects.
- Process special category or criminal offence data on a large scale.
- Systematically monitor publicly accessible places on a large scale, eg CCTV.

22.6. The ICO also requires organisations to carry out a DPIA if they plan to:

- Use innovative technology (in combination with any of the criteria from the European guidelines).
- Use profiling or special category data to decide on access to services;
- Profile individuals on a large scale.
- Process biometric data (in combination with any of the criteria from the European guidelines).
- Process genetic data (in combination with any of the criteria from the European guidelines).
- Match data or combine datasets from different sources.
- Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing').
- Track individuals' location or behaviour (in combination with any of the criteria from the European guidelines).
- Profile children or target marketing or online services at them.
- Process data that might endanger the individual's physical health or safety in the event of a security breach.

22.7. DPIAs should also be carried out or reviewed if significant changes are planned to existing processing. Where a DPIA is required, the trust's DPIA template needs to be completed and submitted with the procurement request form.

22.8. The responsibility for carrying out a DPIA sits with the member of staff responsible for commissioning a new system or software for processing personal data. They will liaise at an early stage with the DPO, who will advise on the requirement for a DPIA and, where applicable, completion of the trust's DPIA template.

23. Closed Circuit Television (CCTV)

23.1. The Trust's academies use CCTV cameras for monitoring their premises and supporting student behavioural policies. There are visible signs showing that CCTV is in operation which provide trust contact information for data subjects.

23.2. Images from systems are securely stored where only a limited number of authorised persons may have access to them.

23.3. The trust may be required to disclose CCTV images to authorised third parties, such as the police, to assist with crime prevention or at the behest of a court order.

24. Freedom of Information

24.1. The Trust has a duty to publish a statement that details how it will meet its duties under the Freedom of Information Act 2000. The Trust has 20 working days to respond to FOI requests (See Appendix 2). The first working day is the day after the request was received. All requests for public information are covered by the Act and FOI may arrive in hard copy format, via email or via social media channels.

24.2. Some requests for information may be received that do not require a formal FOI process to be initiated. An example of this could be a request that can be managed as a normal customer service enquiry and where information is readily available. If in doubt, or should the requestor state the request to be a formal FOI, then this policy must be followed.

24.3. A valid FOI request should be in writing, state the enquirers name and correspondence address and describe the information requested.

24.4. Important points to note:

- Requests should be dealt with within 20 days excluding school holidays.
- All staff should be aware of this process.
- A record should be kept of refusals and reasons for refusals as well as appeals, allowing the governing body to review its access policy on an annual basis.

- Expressions of dissatisfaction should be handled through the school's existing complaints procedure.

24.5. If a member of staff receives a request for information it should be forwarded to CFOO of The Trust, who in turn will:

- Decide whether the request is a request under Data Protection Act 2018 (DPA), Environmental Information Regulations 2004 (EIR) or Freedom of Information Act 2000 (FOIA).
- Decide whether the school holds the information or whether it should be transferred to another body.
- Inform the enquirer if the information is not held.
- Consider whether a third party's interests might be affected by disclosure and if so consult them.
- Consider whether any exemptions apply and whether they are absolute or qualified.
- Carry out a public interest test to decide if applying the qualified exemption outweighs the public interest in disclosing the information.
- If a request is made for a document that contains exempt personal information ensure that the personal information is removed as set out in the guidance for schools.
- Decide whether the estimated cost of complying with the request will exceed the appropriate limit.
- Consider whether the request is vexatious and repeated

24.6. The Trust will endeavour to provide information in the format requested, so long as it is practicable to do so. The Trust will also provide advice and assistance, as far as is reasonable, to any person who proposes to make, or has made, requests for information.

25. Training and Awareness

25.1. Staff on permanent contracts or long-term temporary contracts must read the relevant documents referred to in the Induction Policy, which includes GDPR related policies and procedures, on taking up post. Staff on short-term temporary contracts must be given the GDPR induction briefing immediately on starting their assignment.

25.2. All staff will receive training on data protection on induction and, subsequently, at least annually. Training will be delivered both in person (by the Trust DPO) and digitally.

25.3. Staff must complete an online form to record participation in data protection training. The information submitted will form a record of training and will be used as the basis for a training needs analysis.

26. Contact Details

26.1. Any questions or concerns relating to this policy should be directed to The Legacy Learning Trust's DPO at:

The Legacy Learning Trust
c/o Acklam Grange School
Lodore Grove
Middlesbrough
TS5 8PB

Telephone: 01642 277700
Email: dpo@tllt.org.uk

26.2. Individuals wanting to exercise their right to lodge a complaint with a supervisory authority should contact:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 0303 123 1113 (local rate) or
01625 545 745 (national rate number)
Website: www.ico.org.uk/concerns

27. Appendix 1 – Clear Desk and Screen Requirements

This appendix sets out example of the steps staff must take to ensure that personal information is processed securely. This list is not exhaustive. Key risks associated with unauthorised disclosure include documentation left unattended on desks, printers or photocopiers and electronic information visible on unlocked computer displays. In order to minimise the risks of unauthorised disclosure, staff must take all practical steps:

- To ensure that computer screens are not overlooked when accessing personal information by tilting them away from the view of unauthorised persons. In ground floor work areas, blinds should be closed or PC/Laptop screens, information boards or personal information should be positioned so information cannot be viewed by passers-by.
- To ensure that any documentation containing personal information is not visible to anyone unauthorised to view it, for example, on reception or in classrooms
- When leaving their desk, to lock computer screens and remove documentation from view.
- When working areas are left unattended, including at the end of the working day;
    - To lock office or classroom doors if there is personal information in the room.
    - To switch off computers (or lock them if instructed not to switch off).
    - To remove any documentation (whether it contains personal information or otherwise) from desks to lockable filing cabinets or lockable drawers.
    - To ensure doors and windows are closed.
    - To lock all desk pedestals and cabinets.
    - To secure laptops and mobile devices.
    - To clear all printers and photocopiers of printed material.
    - To wipe clean all white boards and clear flip charts of sensitive data.
    - When using keys to lock doors, cabinets etc to store the keys securely.

28. Appendix 2 – Request Breakdown Table

		How long does the organisation have to respond to be complaint?	Aim to respond time
FOI (Freedom of information)	Comes from a third party. Usually generic, not specific to an individual	20 working days from receipt of request (excluding non-working days, i.e. school holidays)	20 working days from receipt of request (excluding school holidays)
SAR (Subject access request)	Any request for personal data. Can come from anyone we hold information on (Staff, student, parent if child is less than 13 years) *The right to access information you hold about a child is the child's right rather than anyone's else's, even if:* ▪ *they are too young to understand the implications of the right of access;* ▪ *the right is exercised by those who have parental responsibility for the child; or* ▪ *they have authorised another person to exercise the right on their behalf.* *Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the request is from a child and you are confident that the child can understand their rights, you should usually respond directly to the child. You may allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.*	1 calendar month from receipt of request. If date falls on a weekend or bank holiday – the next working day. *You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual, eg other types of requests relating to individuals' rights.* *If you process a large amount of information about an individual, you may be able to ask them to specify the information or processing activities their request relates to, if it is not clear. The time limit for responding to the request is paused until you receive clarification, although you should supply any of the supplementary information you can do within one month.*	1 calendar month from receipt of request. If date falls on a weekend or bank holiday – the next working day.
Educational Record	Request from a parent in relation to a students educational information, regardless of students age (no permission from child needed).	Academies are not obliged to respond to a request for access to a pupils education record under current legislation.	30 working days from receipt of request, excluding school holidays.