DATA PROTECTION POLICY

This policy applies to all schools in The Lionheart Educational Trust

Approved by Trust Board: September 2022 - September 2024

1.0 Introduction

1.1 Lionheart Educational Trust ("the Trust") collects and processes personal data to meet and fulfil a range of functions and statutory obligations as an Academy Trust.

1.2 The Trust is a Data Controller, as defined in Section 1 of the Data Protection Act 2018, and must ensure that all requirements within the Act are implemented, monitored and evaluated.

1.2 The Trust is fully committed to fulfilling all of its legal obligations as well as following best practice guidelines to ensure personal data held is managed securely and compliantly.

1.3 This policy sets out how the Trust will manage personal data in accordance with the Data Protection Act 2018 and the UK GDPR, and specifies the standards expected by the Trust in processing personal data and the safeguarding individuals' rights and freedoms.

2.0 Scope

2.1 This policy applies to all members of staff within the Trust. For the purposes of this policy, the term "staff" means all members of Trust staff including permanent, fixed term, and temporary staff, governors, secondees, any third-party representatives, agency workers, volunteers, interns, agents and sponsors engaged with the Trust in the UK or overseas. This policy also applies to all members of staff employed by any of the Trust's subsidiary companies.

2.2 This policy applies to all personal data and sensitive personal data processed by the Trust, regardless of whether this is in paper or electronic format.

2.3 All staff must comply with this policy when processing personal data on behalf of the Trust. Any breach of this policy may result in disciplinary action.

3.0 Definitions

3.1 **Data Controller**: An organisation that has control of and determines the processing of personal data and/or sensitive personal data

3.2 **Data Subject**: A living and identifiable individual who is the subject of personal data

3.3 **Data Processor**: Any person or organisation who processes the data on behalf of the data controller

3.4 **Personal Data**: Any information which relates to a living individual who can be identified from the information. This includes any expression of opinion about the individual.

3.5 **Personal Data Breach**: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to personal data transmitted, stored or otherwise processed.

3.6 **Sensitive Personal Data**: Also known as special category data and criminal offence data (GDPR). Includes data that falls into one of the following categories below:

- Ethnicity
- Gender
- Religious or other beliefs
- Political opinions

- Membership of a trade union
- Sexual life
- Physical and mental health
- Offences committed or alleged to have been committed by that individual

3.7 **Third Party**: Any person or organisation other than the data subject, data controller or data processor.

4.0 Roles and Responsibilities

4.1 Trust Board

The Trust Board have overall responsibility for ensuring that Lionheart Educational Trust complies with all relevant data protection obligations.

4.2 Trust Leadership Team

The Trust Leadership Team are accountable to the Trust Board for ensuring there are appropriate standards established across the Trust for managing personal data which are monitored and regularly reviewed.

4.2 Heads of School

Heads of School are accountable for the day to day security and compliance of personal data processed by staff within their schools, ensuring that Trust level standards are being effectively followed and that emerging risks are highlighted to the Corporate Information Governance Group.

4.3 Senior Information Risk Owner (SIRO)

The Trust's SIRO is responsible for overseeing a framework to continually assess risks to information across the organisation and implementing corrective policy changes and best practice. The SIRO will oversee the investigation of security incidents or personal data breaches which may involve notification to the ICO, and for approving disclosures of personal data outside of the organisation which do not fall within established data sharing agreements.

4.4 Information Compliance Group (ICG)

The primary function of the ICG is to oversee, and provide leadership for the efficient and effective management of information within the Trust including all schools and colleges. Chaired by the SIRO, the ICG will act as the primary decision-making authority for the development of standards and best practice and act as a point of escalation for all data compliance and security matters.

4.5 Data Protection Officer (DPO)

The DPO is responsible for monitoring compliance and ensuring controls and measures are established and followed. Key areas of responsibility include reviewing and updating policies, privacy notices and related guidance; providing specialist advice on data protection issues, including breaches; maintaining Records of Processing Activities (ROPA); acting as the single point of contact with the ICO and advising on changes to the risk profile. The DPO is an independent role to advise and make recommendations to the Trust, and reports directly to the SIRO.

4.6 Chief Information Security Officer (CISO)

The Chief Information Security Officer is responsible for ensuring the technical security and protection of the Trust's information assets, and for maintaining appropriate levels of

certification to demonstrate security measures in place. Reporting directly into the SIRO, the CISO is responsible for:

- Protection of Trust assets from attacks and data loss;
- Advising on emerging risks and recommended mitigations;
- Maintaining certifications.

4.7 Information Asset Owners

All information assets identified within the Information Asset Register will be assigned to an Information Asset Owner. Information Asset Owners are responsible for:

- ensuring the ongoing integrity and security of data held within the information asset;
- assisting with an incidents or breach investigations with relate to that information asset;
- escalating any risks to the data held within the information asset to the ICG.

4.8 Line Managers

Line Managers are responsible for ensuring staff under their management are informed of this policy and have completed all mandatory data protection training annually, as well as any additional training relevant to their job role.

4.9 Staff

All staff who process personal data are responsible for:

- adhering to the requirements laid down in this policy;
- completing all mandatory data protection training as well as any refresher training;
- managing personal data securely in accordance with established practices and procedures;
- reporting suspected or confirmed data breaches promptly and without delay.

5.0 The Data Protection Principles

5.1 The Trust expects all staff handling personal data to abide by the Data Protection Principles, as outlined below:

Personal Data shall be:

i. processed **lawfully**, **fairly** and in a **transparent manner** in relation to individuals;

ii. **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;

iii. **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;

iv. **accurate and, where necessary, kept up to date**;

v. 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; and

vi. 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

5.2 In addition the Trust is required to demonstrate compliance for how it is processing personal data. This is referred to as the Accountability Principle, or Seventh Data Protection Principle.

The Trust will evidence how it is compliant through its policies and procedures and through documenting all processing activities.

6.0 How the Trust applies the Data Protection Principles

6.1 The Trust will only process personal data where we have one of six 'lawful basis' (legal reasons) to do so:

i. The individual (or their parent/carer) has freely given clear consent

ii. The data needs to be processed so that the Trust can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract

iii. The data needs to be processed so that the Trust can comply with a legal obligation

iv. To ensure the vital interests of the individual e.g. to protect someone's life

v. The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions

vi. The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)

6.2 The Trust will publish privacy notices to explain what personal data is collected and processed and the nature of this processing. Privacy notices will include the identity of third parties to whom we may share, disclose or be required to pass on information to, whilst accounting for any exemptions which may apply under the Act.

6.3 The Trust will only process special category data where an additional special category condition has been identified.

6.3 The Trust will publish an Appropriate Policy Document, detailing what Special Category and Criminal Offence data the Trust processes, the lawful basis for processing it, the purposes for which it is processed, and how it is processed compliantly with the data protection principles.

6.4 The Trust will maintain Record of Processing Activities (ROPA) for each School and college to demonstrate the purposes and lawful basis for the personal data it processes.

6.5 Where personal data is collected on the basis of consent, records of consent provided will be maintained. The Trust will ensure consent can be withdrawn easily at any time.

6.6 When obtaining personal data staff must ensure that the purpose under which they are collecting the data is included in the Trust's web-based privacy notice. If it is not they should notify the Data Protection Officer so that this can be reviewed.

6.7 The Trust will issue all data subjects with a privacy notice at the point at which their personal data is collected. Where personal data which is obtained indirectly a privacy notice will be communicated to the data subject within at least one month of receiving the data.

6.8 Schools must ensure that mechanisms are put in place for keeping personal data accurate and up to date where this is necessary. Student contact details should be verified by Schools at least once per academic year.

6.9 Access to personal data must be restricted to staff who need to access the information in the course of their duties. An Information Asset Register will be maintained by each school to list key data assets and document how they are kept secure.

6.10 The Trust will ensure that all personal data is securely disposed of once no longer required in line with the Trust's retention policy. The Trust has adopted the Information and Records Management Society retention schedule within the Records Management Policy.

6.11 The Trust will establish data sharing agreements where personal data is routinely shared outside of the organisation for specified and lawful purposes. Where the request does not fall within a routine disclosure, the Trust will ensure an appropriate external data sharing form is completed to assess the disclosure prior to any data sharing being made; unless the request is to protect the vital interests of that individual, and disclosure needs to be made immediately.

6.12 When procuring a new system or service which will involve a third-party processing Personal Data on our behalf, we will take steps to ensure the Data Processor provides sufficient guarantees of their technical and organisation measures for data protection by design. The Trust will ensure that Data Processing Agreements are entered into whenever the Trust contracts out processing of personal data to third parties (data processors).

6.13 The Trust will not transfer or share personal information with countries outside of the European Economic Area (EEA) unless that country has a recognised adequate level of protection in place in line with the recommendations outlined in the Act.

6.14 The Trust will ensure all staff are provided with data protection training appropriate to their job role, and promote the awareness of the Trust's data protection and information security policies, procedures and processes.

6.15 The Trust understands its responsibilities around data security and will ensure that policies and systems are in place to provide the highest level of protection to personal data held. To help fulfil this obligation the Trust will obtain certification via the Cyber Essentials scheme.

6.16 The Trust will complete Data Protection Impact Assessments (DPIAs) for all new processing activities involving personal data, or which involve significant changes to existing data processing activities.

7.0 Data Protection Impact Assessments (DPIA)

7.1 DPIA must be undertaken before the processing of any personal data which is "likely to result in a high risk to the rights and freedoms" of individuals. It is the Trust policy that a DPIA is completed for any project involving the processing of student personal data.

7.2 Where it is concluded that a DPIA is unnecessary and will not be undertaken, the reasons for this will be clearly documented. This will ensure a clear audit trail for the decision is maintained by the Trust for accountability purposes.

7.4 Where the outcome of a DPIA is that the processing of personal data would result in a high risk, and it is not possible to take any measures to eliminate or mitigate that risk, the Information Commissioner's Office (ICO) will be consulted by the Data Protection Officer.

8.0 Data Subjects Rights

8.1 The Trust acknowledges data subjects' right to access personal data held on our systems and in our files upon their request, or to delete and/or correct this information if it is proven to be inaccurate, excessive or out of date.

8.2 The Trust is fully committed to facilitating access by data subjects ("applicants") to their personal data, while bearing in mind the need to protect other individuals' rights of privacy.

8.3 All applicants are encouraged to fill in a Subject Access Request form when requesting access to their personal data.

8.4 Applicants who are not members of the Trust must submit supporting documentation which establishes that they are the data subject (or where the application is made by a third party on behalf of the data subject, which establishes the third party's identity, that of the data subject and a form of authority signed by the data subject is produced).

8.5 The Trust will respond to all requests within the statutory time period of one calendar month.

8.6 The Trust recognises that individuals have the right to prevent data processing where it is causing them damage or distress, or to opt out of automated decision making and stop direct marketing.

8.7 The Trust reserves the right to withhold information from a Subject Access Request or elements of a Subject Access Request if the information requested is determined to be exempt from disclosure under the Data Protection Act 2018.

9.0 Parental Rights

9.1 The Data Protection Act 2018 provides that children and young adults can assume control over their personal information and restrict access to it from the age of 13 where they are deemed mature enough to understand their rights.

9.2 Requests from students aged 13 and above to restrict access to personal data will be considered on a case by case basis.

9.3 Requests for restricted parental access will generally not be granted where the student is living with that parent.

9.4 The Trust acknowledges that all parents have a legal obligation to ensure that a child of compulsory school age receives a suitable full-time education (ACT). The Trust will ensure that an educational record containing the student's progress and attainment in the main subject areas taught is provided to the parents of each registered student, regardless of whether access to other personal data has been restricted.

10.0 Photographs and Videos

10.1 Processing for Domestic Purposes

Families and guests attending Trust events may be allowed to take photographs and videos for domestic purposes where it is deemed safe and appropriate to do so. If photographs are taken for personal use they are not covered by the Act.

10.2 The Trust does not endorse photographs or videos collected for domestic purposes to be used for any other purpose. Images or videos which include other students should not be posted on any social media or other public facing channel unless consent from the data subjects has been sought.

10.3 The Head of School, or other delegated person responsible, will always advise whether permission is granted for families and guests to take photographs at events. There may be circumstances where permission is not granted where there are identified concerns or risks to individuals. Families and guests are requested to respect the final decision of the school.

10.4 Processing for Official Use

The Trust will collect photographs of staff and students for security and identification purposes. The Trust does not require consent for this type of processing.

10.5 Processing based on consent

Images captured for marketing purposes and to 'celebrate life at school' for both staff and students are processed under the legal basis of consent. Consent will be sought from either the data subject or where relevant the parents/carers of the data subject.

Once an image has been published with consent, it will not always be possible for the Trust to remove the image from public display should consent be withdrawn, although the image will be removed from further distribution.

The Trust will ensure that any images captured adhere to its safeguarding policy. The Trust will not display a child's full name alongside their image in any areas of the school or media, without written permission from parents/carers.

11.0 Data Breaches

11.1 All suspected or confirmed personal data breaches must be reported immediately in accordance with the Data Breach Procedure.

11.2 The Trust will maintain a log of all breaches identified by the Trust.

11.3 All reported data breaches will be investigated immediately and where necessary they will be notified to the data subject and to the Information Commissioners Office within 72 hours.

12.0 Related Policies, standards and guidelines

12.1 The Data Protection Policy should be read in conjunction with the following other Trust policies:

- Appropriate Policy Document
- Data Breach Procedure
- Data Protection compliance Statement
- CCTV Policy
- Biometric Data Policy
- Electronic Communication Policy
- Records Management Policy

13.0 Review

13.1 The Data Protection Officer will be responsible for ensuring that this policy and its associated procedures are reviewed bi-annually. Changes will be ratified by the Trust board.

13.2 Date of next review: September 2024