



## **DATA PROTECTION POLICY**

**This policy applies to all the academies in  
The Lionheart Academies Trust**

<b>Version</b>	<b>Document History</b>	<b>Date</b>
Version 1.0	Initial Document	01/07/2014
Version 2.0	Approved by Board and issued to all schools	17/05/2016
Version 3.0	Approved by Board and issued to all schools	01/05/2018

Signed by Chair of Board: \_\_\_\_\_



## **1.0 Purpose**

1.1 The General Data Protection Regulations 2018 ('the Act') has two principal purposes:

- i) to regulate the use by those who obtain, hold and process personal data on living individuals (known as data controllers) and;
- ii) to provide certain rights (for example, of accessing personal information) to those living individuals (known as data subjects) whose data is held.

1.2 The cornerstones of the Act are the six data protection principles, which requires that 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; 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;
- 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; 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;
- 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; 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 act in order to safeguard the rights and freedoms of individuals; 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

## **2.0 Policy**

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

2.2 The LAT is fully committed to abiding, not only by the letter, but also by the spirit of the Act, and, in particular, is committed to the observation, wherever possible, of the highest standard of conduct mandated by the Act. This policy has been written to acquaint staff with the duties under the Act and to set out the standards expected by the LAT in relation to processing of personal data and safeguarding individuals' rights and freedoms.

2.3 All contractors and agents acting for or on behalf of the LAT should be made aware of this policy.

2.4 This policy applies to all personal data and sensitive personal data processed on computers and stored in manual (paper based) files. It aims to protect and promote the rights of individuals and the LAT.



(i) Personal Data: Any information which relates to a living individual who can be identified from the information. It also extends to any information which may identify the individual. Examples of personal data:

- A person's name and address (postal and email)
- Date of birth
- Statement of fact
- Any expression or opinion communicated about an individual
- Minutes of meetings, reports
- Emails, file notes, handwritten notes, sticky notes
- CCTV footage if an individual can be identified by the footage
- Employment and student applications
- Spreadsheets and/or databases with any list of people set up by code or student/staff number
- Employment or education history

(ii) Sensitive Personal Data: Any information relating to an individual's:

- Ethnicity
- Gender
- Religious or other beliefs
- Political opinions
- Membership of a trade union
- Sexual orientation
- Medical history
- Offences committed or alleged to have been committed by that individual

2.4 Employees of the LAT are expected to:

- acquaint themselves with and abide by, the Data Protection Principles;
- read and understand this policy document;
- understand how to conform to the standard expected at any stage in the life-cycle;
- understand how to conform to the standard expected in relation to safeguarding data subjects' rights (e.g. the right to inspect personal data) under the Act;
- understand what is meant by 'sensitive personal data', and know how to handle such data;
- contact the Data Controller if in any doubt, and not to jeopardise individuals' rights or risk a contravention of the Act.

### 3.0 Definition

3.1 The General Data Protection Regulations 2018 is designed to protect individuals and personal data, which is held and processed on their behalf. The Act defines the individual as the 'data subject' and their personal information as 'data'. These are further defined as:



(i) **Data Subject:** Any living individual who is the subject of personal data whether in a personal or business capacity

(ii) **Data:** Any personal information which relates to a living individual who can be identified. This includes any expression of opinion about the individual.

(iii) Data is information stored electronically i.e. on computer, including word processing documents, emails, computer records, CCTV images, microfilmed documents, backed up files or databases, faxes and information recorded on telephone logging systems

(iv) Manual records which are structured, accessible and form part of a 'relevant filing systems' (filed by subject, reference, dividers or content), where individuals can be identified and personal data easily accessed without the need to trawl through a file.

#### 4.0 The Data Protection Principles

4.1 The General Data Protection Regulations 2018 sets legislative requirements for organisations processing personal data (referred to under the Act as 'Data Controllers'). The LAT will be open and transparent when processing and using private and confidential information

4.2 When processing personal data and sensitive personal data the LAT will use the following lawful bases for processing:

Data Type	Lawful bases for Processing
Student Data	Legal obligation
Parent Data	Legal obligation
Staff Data	Contractual obligation
Maths Hub Data	Contractual obligation
Community Groups who use LAT Sites	Contractual obligation
Information Used for Marketing and Community Engagement	Consent

4.3 The LAT will issue all data subjects a privacy notice within one month of receiving the data.

4.4 The LAT recognises and understands the consequences of failure to comply with the requirements of the Act which may result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;
- Suspension/withdrawal of the right to process personal data by the Information Commissioners Office (ICO);
- Loss of confidence in the integrity of the LAT's systems and procedures;
- Irreparable damage to the LAT's reputation.

4.5 The LAT may also consider taking action, in accordance with the LAT's Disciplinary Procedure, where staff do not comply with the Act.



## **5.0 Roles and Responsibilities**

- 5.1 Staff will not attempt to gain access to information that is not necessary to hold, know or process. All information which is held will be relevant and accurate for the purpose for which it is required. The information will not be kept for longer than is necessary and will be kept secure at all times.
- 5.2 The LAT will ensure that all personal or sensitive personal information is anonymised as part of any evaluation of assets and liability assessments except as required by law.
- 5.3 Staff who manage and process personal or sensitive personal information will ensure that it is kept secure and where necessary confidential. Sensitive personal information will only be processed fairly and lawfully and in line with the provisions set out in the Act and only processed in accordance with instructions set out by the respective Data Controllers.
- 5.4 The LAT will ensure that all staff are made aware of the reasons why personal and sensitive personal data is being processed:
- how it will be processed
  - who will process it
  - how it will be stored and
  - how it will be disposed of when no longer required.

## **6.0 Data Subjects Rights**

- 6.1 The LAT acknowledges individuals (data subjects) rights under the Act to access any 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.
- The LAT 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.
- 6.2 All applicants will be expected to fill in a Subject Access Request form, available from the LAT if needed. Applicants who are not members of the LAT 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).
- 6.3 The LAT recognises that individuals have the right to make a request in writing and without a fee, obtain a copy of their personal information, if held on our systems and files. The LAT will provide the information within 20 working days.
- 6.4 The LAT 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.

## **7.0 LAT Obligations (Data Controllers)**

- 7.1 The LAT will follow the Code of Practice issued by the ICO when developing policies and procedures in relation to data protection.
- 7.2 The LAT will ensure that Data Processing Agreements are applied to all contracts and management agreements where the LAT is the data controller contracting out services and processing of personal data to third parties (data processors). The LAT will ensure this agreement clearly outlines the roles and responsibilities of both the data controller and the data processor.

- 7.3 The LAT will adhere to and follow the principles of data protection when conducting surveys, marketing activities etc., where the LAT collects, processes, stores and records all types of personal data.
- 7.4 The LAT 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.
- 7.5 The LAT will ensure all staff are provided with data protection training and promote the awareness of the LAT’s data protection and information security policies, procedures and processes.
- 7.6 The LAT understands its responsibilities around data security and will ensure that policies and systems are in place to provide the highest level of protection. To help fulfil this obligation the LAT will obtain certification via the Cyber Essentials scheme.

**8.0 Online Data Collection**

- 8.1 The LAT uses Google Analytics to manage data collected from our online services. Google Analytics anonymises this data to ensure that no personal identifiable data is collected.
- 8.2 The LAT does not use any automated tools to make decisions regarding personal data.
- 8.3 On our websites we use cookies to ensure that we give you the best experience when visiting our website. This includes cookies from third party social media websites if you visit a page which contains embedded content from social media. Such third party cookies may track your use of our website. If you continue without changing your settings, we'll assume that you are happy to receive all cookies. However, you can change your cookie settings at any time. Providing that no changes are made the maximum life of a cookie issued from a LAT website will be six months, measured from the date of issue.

**9.0 Data Retention**

- 9.1 The LAT recognises the need to balance the right of data subjects with the legal requirement for data security and retention. The LAT will apply the following retention rules to data it holds:

Category	Description	Maximum Retention Period
Student Personal Data	Contact information for students	7 years after student leaves
Student Sensitive Data	Information on gender, ethnicity, religion and medical information	7 years after student leaves
Staff and Student Core academic data	Transcript like information and basic verification information relating to the individual including accreditations	Perpetuity
Reference data in addition to core academic data	Contents of student file e.g. attendance date, e-mails etc.	7 years after student leaves
Safeguarding Data	Data relating to safeguarding incidents	Perpetuity
Parent Personal Data	Contact information for parents	7 years after student leaves
Staff Personal Data	Contact information for staff	7 Years after staff leaves employment



Staff Sensitive Data	Information on gender, ethnicity and religion	7 Years after staff leaves employment
Staff Financial Data	Information on salaries and pensions etc.	30 Years after staff leaves employment
Trust and Governors Management Papers	Management information packs created for Trust and Governors meetings	Two academic years
Third Party Financial Data	Invoices, credit checks and bank information etc.	7 Years after document date
Application Data for unsuccessful applicants	Expressions of interest and contact information	6 months after cessation of relationship
Alumni Personal Data	Contact information for former students who register as alumni	6 months after cessation of relationship
Community Groups	Contact information for community users of LAT sites	6 months after cessation of relationship
CCTV Data	Data collected for law enforcement and safeguarding purposes	21 Days from date of the recording
Visitor Data	Name, vehicle registration and photograph of anyone visiting a LAT site, used for safeguarding purposes	1 year from date of the last visit

9.2 The LAT will ensure that all physical documents will be securely disposed of once they are no longer required in line with section 8.1.

## 10.0 Complaints

10.1 Complaints relating to breaches of the Data Protection Act 1998 and/or complaints that an individual's personal information is not being processed in line with the eight principles of data protection will be managed and processed by the LAT's HR Team.

10.2 Complaints will be dealt with in accordance with the LAT's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

10.3 All complaints of dissatisfaction should be addressed to:

The Data Protection Officer  
 Lionheart Academies Trust,  
 C/O Beauchamp College,  
 Ridge Way,  
 Oadby  
 LE2 5TP

Telephone: 0116 2729117

E-mail: [DPO@lionhearttrust.org.uk](mailto:DPO@lionhearttrust.org.uk)



## **11.0 Confidentiality and Information Sharing**

11.1 The LAT will only share information in accordance with the provisions set out in the Act.

11.2 Where applicable the LAT will inform individuals of 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.

## **12.0 Review**

12.1 This policy will be reviewed periodically as it is deemed appropriate, to take account of changes in the law and guidance issued by the Information Commissioner. These reviews will be no less frequently than every two years. The policy review will be undertaken by the Director of IT for the LAT and ratified by the LAT Board.