IT Services

Data Protection Policy

Document title:	Data Protection Policy
Version number:	4.2
Policy Status	Approved
Date of Issue	April 2016
Date to be revised	April 2017

Revision Log (last 5 changes)

Date	Version No	Brief detail of change
Jan 15	1.0	Initial document for review
Mar 15	2.0	Added responsibilities and processes
Mar 15	3.0	Removed non-DP elements of the process
Apr 16	4.0	Redesign
Apr 16	4.1	Data-management structure updated
Aug 16	4.2	References to CCTV updated

Policy

This policy applies to all members of Leigh Academies Trust ("the Trust"). For the purposes of this policy, the term "staff" means all members of staff within the Trust, including permanent, fixed-term and temporary staff. It also refers to governors, any third-party representatives, agency workers, volunteers, interns, agents and sponsors engaged with the Trust. This policy also applies to all members of staff employed by any of the Trust's subsidiary companies.

All contractors and agents acting for or on behalf of the Trust will be made aware of this policy.

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

(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 include:

- 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 and reports;
- Emails, file notes, handwritten notes and sticky notes;
- CCTV footage if an individual can be identified by the footage;
- Employment and student applications;
- Spreadsheets and/or databases containing lists 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.

The Trust recognises and understands that the consequences of failure to comply with the requirements of the Data Protection Act 1998 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 Commissioner's Office (ICO);
- Loss of confidence in the integrity of the Trust's systems and procedures;
- Irreparable damage to the Trust's reputation.

Definitions

The Data Protection Act 1998 is designed to protect individuals' and personal data, which is held and processed by others on their behalf. The Act defines the individual as the 'data subject' and their personal information as 'data'. These are further defined as:

- Data subject: Any living individual who is the subject of personal data, whether in a personal or business capacity;
- Data: Any personal information which relates to a living individual who can be identified. This includes any expression of opinion about the individual;
- 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;
- Manual records which are structured, accessible and form part of a 'relevant filing system' (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.

Anonymised data are individual data records from which the personally-identifiable fields have been removed. Data subjects' identities are not discernable from such data.

Aggregated data are data which are processed to produce a generalised result and from which individuals cannot be identified. This might include data brought together to give a broad understanding of, for instance, whole-school academic grade data presented publicly.

Data controller (DC)

A person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Protection Officer (DPO)

A person who works on behalf of the DC to determine the purposes for which and the manner in which any personal data are, or will be, processed for their academy or specific subject.

Data Processor

In relation to personal data, this means any person (other than an employee or subordinate of the data controller) who processes the data on behalf of the data controller. This means that the person processes data for a purpose and according to a manner determined by the data controller and makes no independent determination of such matters.

Information Asset Owner (IAO)

The Information Asset Owner is a senior member of staff who is the nominated owner for one or more identified information assets within the Trust. IAOs will work closely with the Trust to ensure that there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. IAOs will support the senior information risk owner (SIRO) in their overall information risk-management function.

The IAO will document, understand and monitor:

- What information assets are held and for what purpose;
- How information is created, amended or added to over time;
- Who has access to the information and why;
- The risk to the asset, addressing this risk to provide assurance to the SIRO.

Processing

In relation to information or data, this means obtaining, recording or holding the information or data, or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data;
- Retrieval of, consultation on or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise; or
- alignment, combination, blocking, erasure or destruction of the information or data.

Private Cloud

Private cloud is a particular model of cloud computing that involves a distinct and secure cloud-based environment, hosted within the Trust and providing greater control and privacy. The data is saved in a secure Trust repository.

The additional security offered by this ring-fenced cloud model is the preferred method of storing and processing private data and conducting sensitive tasks.

This service is accessible from anywhere through an app or a web browser. These services are currently Citrix, Filecloud and MIS web interfaces.

Public Cloud

Public cloud is a model of cloud computing, in which data is hosted by a third-party company, providing services to multiple clients using the same shared infrastructure.

The Trust utilises public clouds to make its operations significantly more efficient, with the storage of non-sensitive content, online document collaboration and webmail.

Senior Information Risk Owner (SIRO)

The SIRO takes overall ownership of the organisation's information risk policy and the assessment processes for information risk. The SIRO ensures that the Board and the Accounting Officer are

kept up to date and briefed on all information-risk issues affecting the organisation and reviews and agrees actions in respect of identified information risks.

The DPA's eight data protection principles

The Data Protection Act (DPA) 1998 sets legislative requirements for organisations processing personal data (referred to under the Act as 'data controllers'). The Trust will be open and transparent when processing and using private and confidential information by ensuring we follow the eight data-protection principles for good data handling, which are as follows:

1. Personal data shall be processed fairly and lawfully;

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;

3. Personal data shall be adequate, relevant and commensurate with the purpose or purposes for which they are processed;

4. Personal data shall be accurate and, where necessary, kept up to date;

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;

6. Personal data shall be processed in accordance with the rights of data subjects under the DPA;

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

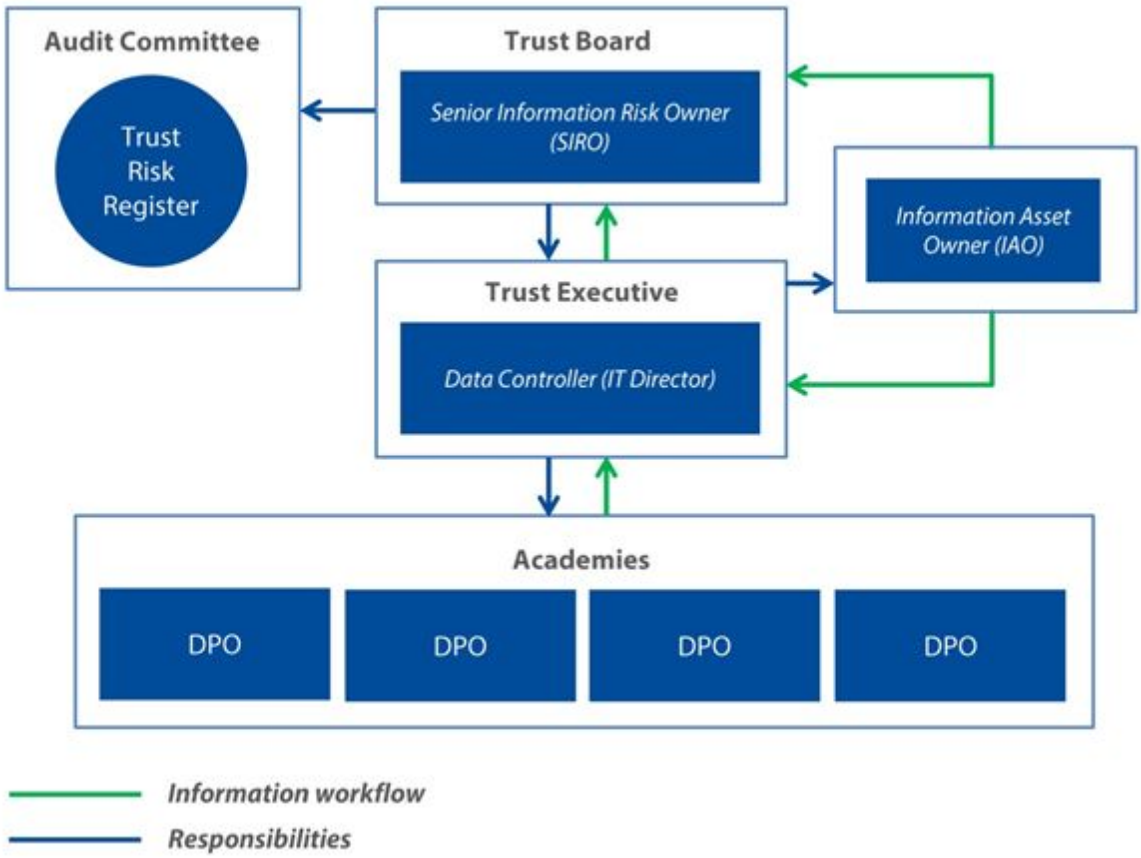
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Responsibilities

It is important that the various parties involved in a data-processing activity establish their roles and responsibilities at an early stage, particularly before the processing commences. This will help to ensure that there are no gaps in organisations' responsibilities.

Under the multi-academy trust (MAT) arrangements, the Trust is responsible for the activities of all the schools in the MAT, even though some functions may have been delegated to local Heads of School or local governing bodies. Providing the schools and academies within the Trust do not have any legal status separate from that of the Trust, the MAT is the legal entity responsible for

the processing of personal data by the schools and the academies within the Trust. The MAT is the data controller for the processing and is subject to DPA registration obligations.



Leigh Academies Trust Data-Protection Governance Structure

The Trust is the data controller (DC) for the purposes of the DPA and the Trust Directors will therefore have overall responsibility for compliance with the DPA. The Directors have delegated this overall responsibility to the Trust IT Director.

The IT Director has delegated responsibility to the Lead Principal in each academy for ensuring compliance with the DPA and this policy within the day-to-day activities of the academy.

For each academy, the Lead Principal will appoint a data-protection officer (DPO). The DPO is responsible for:

- Keeping the SIRO and Trust DC up to date with changes in how the Academy processes data;
- Obtaining consent for disclosure of personal data, including routine consent from parents and pupils for using photographs for general academy purposes;
- Ensuring the use of CCTV is compliant with this policy;
- Ensuring data-protection statements are included on forms that are used to collect personal data;
- Acting as a central point of advice for local staff on data-protection matters;

- Coordinating requests for personal data;
- Arranging appropriate data-protection training for staff;
- Keeping up to date with the latest data-protection legislation and guidance;
- Ensuring staff are following the Trust DP policy and are complying with this policy;
- Ensuring new software or new services for the Academy are compliant with this policy (using the new software request form/privacy-impact assessment).

Staff will not attempt to gain access to information that they do not need to hold, know or process. All information that 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.

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, lawfully, in line with the provisions set out in the Data Protection Act 1998 and in accordance with instructions set out by the appropriate Data Protection Officer.

The Trust 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.

The Trust will ensure that data-processing agreements are applied to all contracts and management agreements where the Trust is the DC, contracting out services and processing of personal data to third parties (data processors). The Trust will ensure these agreements clearly outline the roles and responsibilities of both the DC and the data processor.

Breach of the Policy

Non-compliance with this policy and data-protection legislation by a member of staff is considered a disciplinary matter which, depending on the circumstances, could lead to dismissal.

Data Management

Data Gathering

Whenever an academy collects new information about individuals, the Trust will ensure that individuals are made aware:

- that the information is being collected;
- of the purpose that the information is being collected for;
- of any other purposes that it may be used for;
- with whom the information will or may be shared;
- how to contact the DC.

These requirements encompass the use of CCTV. The Trust will ensure that cameras are in the right place, that they do not breach anyone's privacy and that notices are displayed. The Trust will only obtain relevant and necessary personal data for lawful purposes and will only process the data in ways which are compatible with the purposes for which they were gathered.

Data-protection statements will be included in the prospectus and on forms that are used to collect personal data.

Data Storage

Personal data will be stored in a secure, safe manner. The following measures will be taken to help ensure this:

- Electronic data will be protected through secure passwords, encryption software and firewall systems operated by the Trust;
- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers;
- Manual personal data will be stored securely where it is not accessible to anyone who does not have a legitimate reason to view or process the data;
- Particular attention will be paid to the need for security of sensitive personal data - for example, health and medical records will be kept in a locked cupboard;
- Personal data will not be left in a position where it is visible to unauthorised observers;
- The physical security of academy buildings and storage systems will be reviewed regularly;
- Staff will be trained on this policy and related data-protection procedures.

The only Trust-authorised public cloud, for storage of ***non-sensitive data****, online document collaboration and webmail, is Google Apps For Education (GAFE).* ***No*** *other public cloud or cloud email system, such as Dropbox or Hotmail, should be used for storage of personal and sensitive data.*

Sensitive personal data *should only be accessible through the private cloud and data should be saved internally (not on the public cloud), with the exception of teaching, marking and tracking documents after explicit approval from the Data Protection Officer.*

There is sometimes a slight risk that aggregated data might still allow an individual to be identified - for example, when aggregating a very small group of results, from which other data may be used to identify an individual, even though personal data has been removed. To safeguard data subjects and to manage the Trust's risk, aggregated data, which comprise **no more** than five individual records, should not be used, disclosed or stored in the public cloud without Data Protection Officer (DPO) approval, unless such aggregated data can in no way be matched to identify individual data subjects.

Data Checking

Systems will be put in place to ensure the personal data that the Trust holds is up to date and accurate. (For example, the Trust and its academies will ensure that parents are asked at least once a year to confirm their contact details). Any inaccuracies discovered or reported will be rectified as soon as possible.

Data Disclosure

Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive their data, or to organisations that have a legal right to receive the data without consent being given. When requests to disclose personal data are received by telephone, the

academy will ensure that the caller is entitled to receive the data and will verify their identity. In some circumstances, the academy may call the caller back to check the identity of the caller. Personal data will not be included on the website, in newsletters or in other media without the consent of the individual (or his/her parents where appropriate). Routine consent may be requested from parents to avoid the need for frequent, similar requests for consent being made by academies. Personal data will only be disclosed to the police if they are able to supply a form which notifies of a specific, legitimate need to have access to specific personal data.

Destroying Data

Out-of-date information will be discarded if no longer relevant. Personal data will only be kept for as long as reasonably needed, for legal or business purposes.

We retain day to day CCTV images for 31 days. After 31 days, the only images that are retained are those images which the Trust have identified relate to the following purposes:

- Prevention and investigation of crime
- Prosecution of offenders
- Safety of employees, pupils and members of the public

Data Subjects' Rights

The Trust acknowledges individuals' (data subjects') rights, under the DPA, to access any personal data held on our systems and in our files upon their request, or to ensure that this personal data is deleted and/or corrected if it is proven to be inaccurate, excessive or out of date.

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.

Data Subject Access Requests

Any person whose personal data is held by the Trust is entitled, under the DPA, to ask for access to this information. The request must be in writing. The right is to view or be given a copy of the personal data, rather than to view the whole document containing the personal data. There are some exceptions to this right of access - e.g., in relation to examination scripts or legal advice. When a request is received by a member of staff, this should be passed to the academy's Data Protection Officer without delay. The request must be dealt with promptly; a response must be provided as soon as possible and no later than 40 calendar days from the date on which the request was received.

The Trust may make a charge of £10 for responding to a request for personal data under the DPA and will need to confirm the requester's identity. In relation to requests to view CCTV footage, specific information will be required about the details of the incident (location, approximate time, type of clothing worn, etc).

Parents can make data-subject access requests on their child's behalf, if their child is deemed too young to look after their own affairs. If a request is made by a parent for personal data relating to their child and the child is aged 12 years or older, written consent will need to be sought from the child before the data is disclosed to the parent. A record will be kept of all data subject access requests made that require formal consideration.

Permission to view CCTV footage is granted on the basis that only the data subject can view the footage. Under the Data Protection Act, it is not permissible for the data subject to bring anyone else into the viewing room to view the footage with them.

Please note that although the data subject may be given consent to view CCTV footage, it may not always be possible to give you a copy in any format of the related footage. The decision will be based entirely on the circumstances of the event.

Contact Information

Data Protection Registration No: **ZA102682**

Leigh Academies Trust, Data Protection Controller:
Data Protection Controller
Leigh Academies Trust
Green Street Green Road
Dartford
Kent
DA11QE

datacontroller@latrust.org.uk