LEARNING ALLIANCE ACADEMY TRUST
DATA PROTECTION POLICY

This policy should be read in conjunction with the Data Protection Act 2018 (DPA), the Education Pupil (Information) Regulations 2005, Independent School Standards Regulations 2010 (these apply to academies) and the Information Commissioner's Office (ICO) 'Report on the data protection guidance we give schools 2012' and the Protection of Freedoms Act 2012.

Introduction

The Learning Alliance Academy Trust acknowledges that to function properly we need to collect and use certain types of information about staff, students and other individuals who come into contact with the school. We are also obliged to collect and use data to fulfil our obligations to the local authority (LA), DFE and other bodies. We deal with information properly in whatever way it is collected, recorded and used – on paper, electronically, in the 'cloud' or any other way. We regard the lawful and correct treatment of personal information as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. We are conscious that much of the data we hold is classified as sensitive personal data and we are aware of the extra care this kind of information requires. We ensure that our organisation treats all personal information lawfully and correctly. To this end, we fully endorse and adhere to the data protection principles as contained in the Data Protection Act 2018.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics

	• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Data protection principles

All members of staff employed in our trust are required to adhere to the eight enforceable data protection principles as set out in the Data Protection Act 2018.

- Data shall be processed fairly and lawfully and in particular shall not be processed unless specific conditions are met.
- Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and where necessary, kept up-to-date.
- Personal data shall not be kept for longer than is necessary for that purpose or those purposes.

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

- 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 whether it is held internally or cloud based.

- 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.

Cloud services
We as a Trust we are responsible for:

- Ensuring that the processing carried out by our cloud service provider complies with the DPA requirements by means of a contract and data processing agreement.

- Ensuring the accuracy of the self-certification statements made by the cloud services suppliers by using the self-certification checklists facilitated by the DFE.

School practice

Within the Trust we will strictly apply the following criteria and controls. These are to:

- Notify the ICO that we process personal data and re-notify if procedures change or are amended.

- Observe fully the conditions regarding the fair collection and use of information. To achieve this we have in place and use a privacy notice which may differ according to the data subject concerned.

- Meet our legal obligations to specify the purposes for which information is used.

- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.

- Ensure the quality of information used.

- Apply strict checks to determine the length of time information is held.

- Ensure that the rights of the persons about whom information is held can be fully exercised under the Act. These include the right to be informed that processing is being undertaken, the right to access one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information.

- Take appropriate technical and organisational security measures to safeguard personal information. We will review the physical security of buildings and storage systems as well as access to them. All portable electronic devices must be kept as securely as possible on and off school premises.

- Ensure that all Disclosure and Barring Service (DBS, formerly Criminal Records Bureau) records (recruitment and vetting checks) are kept in a safe central place and that no unnecessary certification information is kept longer than six months.

- Ensure that personal information in not transferred abroad without suitable safeguards.

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- Set out clear procedures for responding to requests for information – see appendix 1.
- Have in place secure methods for safely disposing of all electronic and paper records.
- Be sure that photographs of pupils are not included in any school publication or on the school website without specific consent.
- Ensure that biometric data concerning pupils are not obtained or used without the knowledge of the child and parents and without permission being obtained from them as appropriate.
- Take care that CCTV that captures or processes images of identifiable individuals is done in line with the data protection principles.

We shall also ensure that:

- There is a named person with specific responsibility for data protection within the school. This is currently Michele Cawte.
- All persons managing and handling personal information understand that they are contractually responsible for following good data protection practice.
- All persons managing and handling personal information are trained to do so.
- Anyone wanting to make enquiries about handling personal information knows what to do.
- Anyone managing and handling personal information is appropriately supervised.
- Queries about handling personal information are properly and courteously dealt with.
- Methods of handling personal information are clearly described.
- A regular review and audit is made of the way personal information is held, managed and used.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- A breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against the members of staff concerned.
- On occasions when information is authorised for disposal, it is done appropriately.

Appendix 1

Dealing with a subject access request

- Requests for information must be made in writing (which includes the use of e-mail) and be addressed to the Executive Headteacher. If the initial request does not clearly specify the information required, then the school will make further enquiries.

- The Executive Headteacher must be confident of the identity of the individual making the request. When the request concerns data about a pupil, checks will also be carried out regarding proof of relationship to the child. In addition, evidence of identity will be established by requesting production of:

    - Passport.

    - Driving licence.

    - Utility bills with the current address.

    - Birth/marriage certificate.

    - P45/P60.

    - Credit card or mortgage statement (this list is not exhaustive).

- As stated above, any individual has the right of access to information held about them. However, in the case of children this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Executive Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent, an individual with parental responsibility or guardian shall make the decision on behalf of the child.

- The response time for subject access requests, other than for educational records, is 40 days from receipt (this refers to calendar days irrespective of school holiday periods).

- The DPA allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

- Third party information is information that has been provided by another person such as the LA, the police, a health care professional or another school. It is normal good practice to seek the consent of the third party before disclosing information. Even if the third party does not consent, or consent is explicitly not given, the data may be disclosed. (There is no need in the case of third party requests to adhere to the 40-day statutory timescale.)

- Any information that could cause serious harm to the physical, emotional or mental health of a pupil or another person may not be disclosed, nor should information that would reveal that the child is at risk of abuse. The same stricture applies to information relating to court proceedings.

- If there are concerns about the disclosure of information, then additional advice should be sought, usually from the Information Commission's Office.

- When redaction (blacking out or obscuring of data) has taken place, then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

- Information disclosed should be clear, with any codes, technical terms, abbreviations or acronyms explained. If information contained within the disclosure is difficult to read or illegible, it will be retyped.

- Information can be provided at the school with a member of staff on hand to assist if requested, or provided at face-to-face handover. The views of the applicant will be taken into account when considering the method of delivery. If postal systems have to be used, then registered or recorded mail will be used.

- Complaints will be dealt with in accordance with the school complaints procedure, which is available on-line or from the school office. Should the complainant wish to take the matter further, it may be referred to the Information Commissioner www.ico.gov.uk.

- This policy will be reviewed by the Executive Headteacher at least every two years.