



Data Protection Policy

Leeds East Primary Partnership – A Co-operative Trust

Approved by the Trust Board July 2026

To be reviewed 2027

1. Aims

The Leeds East Primary Partnership (LEPP) aims to ensure that all personal data about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR, the provisions of the DPA 2018 and the Data (use and Access) Act 2025. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#).

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data. It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, living individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none">• 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,

	<p>recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
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.

4. The data controller

LEPP processes personal data relating to pupils, staff, trustees, visitors and others, and therefore is a data controller along with the partner schools and is registered as a data controller with the ICO and will renew this registration and pay the appropriate fee annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by LEPP directly and partner schools and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust Board

The board has overall responsibility for ensuring that LEPP complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will report their activities via the Trust Administrator to the board and, where relevant, report to the board their advice and recommendations on data protection issues.

The DPO will also be the first point of contact for individuals whose data LEPP processes, and for the ICO.

Our DPO is Bywater Kent Support Services Limited and is contactable by email DPO@bywaterkent.co.uk.

5.3 The Trust Chair

The Chair acts as the representative of the data controller on a day-to-day basis.

5.4 All staff (LEPP and partner schools where appropriate)

Staff and trustees are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.

- Informing LEPP of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that we must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how LEPP aims to comply with these principles.

7. Collecting personal data

7.1 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in line with the Information Management Society's Toolkit For Schools.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our trustees.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9.0 Artificial Intelligence (AI)

9.01 AI tools are now common and easy to use. Staff, students, and parents may be familiar with generative AI chatbots like ChatGPT and Copilot, the school understands that AI can help students learn, but it also has risks for personal and sensitive information. To keep this information safe, no one is permitted to enter personal or sensitive data into unauthorised AI tools or chatbots. If anyone does enter such data into an unauthorised generative AI tool, ALPT will treat it as a data breach and will follow the procedures for handling personal data breaches.

10. Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that LEPP holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should preferably be submitted in writing, either by letter, email or fax to the Chair of LEPP or to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately notify the chair and the DPO.

10.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

10.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11. Photographs and videos

As part of our activities, we may take photographs and record images of individuals within our partner schools. We rely on the written consent provided to partnership schools from parents/carers for photographs and videos to be

taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- In school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available our name and contact details and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- Passwords that are at least 8 characters long containing letters and numbers are used to access Trust or partner school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

We will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure published by the ICO. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the website
- Safeguarding information being made available to an unauthorised person
- The theft of a laptop containing non-encrypted personal data about pupils

16. Training

All staff (directly employed by the Trust and by the governors of partner schools) are provided with data protection training as part of their induction process and appropriate refresher training in line with the ICO recommendations.

17. Making and Handling Complaints about Personal Data

In accordance with Section 164a of the Data (Use and Access) Act 2025 schools are now required to include information on how to raise a complaint relating to data protection – see below.

How to Make a Data Protection Complaint

- **Your Right to Complain**
You have the right to make a complaint if you believe school have handled your personal data in a way that breaches the UK GDPR or Part 3 of the Data Protection Act.
- **How to Make a Complaint**
A complaint can be made using the template form in Appendix 1, this is also available directly from LEPP. Once complete, this should be submitted to LEPP at sarah.hay@leedseastprimarypartnership.co.uk.
- **Acknowledging a Complaint**
The school will acknowledge receipt of a complaint within **30 days**.
- **Responding to a Complaint**
Complaints will be investigated as quickly as possible and without undue delay, this will include taking the necessary steps to investigate and deal with any concerns.

- **Keeping You Informed**

As part of handling your complaint, we may make enquiries to better understand what has happened and keep you updated on the progress of our investigation. Once complete, you will be informed of the outcome.

- **Escalation to the ICO**

If a complaint is not resolved by the DPO, the data subject can escalate it to the Information Commissioner for further investigation.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed at least **every two years** in line with [Department for Education's advice on statutory policies](#) and will present to the Trust Board for approval.