Education Partnership Trust

Creating outstanding schools which transform learning, lives and communities

DATA PROTECTION POLICY

Document Control

This document has been approved for operation within:	All Trust Establishments
Date effective from	June 2025
Date next review due by	June 2027
Review period	Biennial

CONTENTS

1.0 INTRODUCTION

1.1 Education Partnership Trust collects, holds and processes personal data about pupils, staff, parents/carers, governors, visitors and other individuals who have contact with the school. It therefore has a number of legal obligations under the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

1.2 Within this policy we will set out how we seek to protect personal data and ensure that employees understand the rules governing their use of personal data to which they have access in the course of their employment. This policy applies to all personal data, regardless of whether it is held in paper or electronic format.

1.3 The school is a registered data controller with the Information Commissioner and will continue to abide by the new registration arrangements. All members of staff have responsibility for how the school collects, holds and processes personal data. The policy therefore applies to all staff as well as external organisations or individuals processing data on behalf of the school. Staff who do not comply with this policy may face disciplinary action.

1.4 This policy also commits that the school will also comply with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, the Protection of Freedoms Act 2012 when referring to use of biometric data and Article 8 of the Human Rights Act 1998.

2.0 DEFINITIONS

2.1 The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

2.2 The GDPR refers to sensitive personal data as 'special categories of personal data'. Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation, are all 'special categories of personal data'.

2.3 The GDPR applies to 'controllers' and 'processors. The school is a data controller who determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller.

3.0 PRINCIPLES

3.1 Under Article 5 of the GDPR, the data protection principles set out the main responsibilities for organisations. It states personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- 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

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 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
- 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 GDPR in order to safeguard the rights and freedoms of individuals
- 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."

3.2 Article 5(2) requires that:

- "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

4.0 LAWFUL PROCESSING

4.1 The first principle requires that organisations process personal data in a lawful manner. The school will only process personal data if it can meet one of the following lawful bases set out under Article 6:

- Consent: the individual has given clear consent for us to process their personal data for a specific purpose
- Contract: the processing is necessary for a contract us have with the individual, or because they have asked us to take specific steps before entering into a contract
- Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations)
- Vital interests: the processing is necessary to protect someone's life
- Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law
- Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests

4.2 In addition, if the school wishes to process 'special category data', it will identify an additional condition for processing as set out under Article 9.

Special Category conditions

- The individual has given explicit consent to the processing for one or more specific Purposes
- Processing is necessary for the Purposes of carrying out the obligations and exercising specific rights of the Controller or of the individual in the field of employment and social security and social protection law so far as it is authorised by Union or Member State law or a collective

agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the individual

- Processing is necessary to protect the vital interests of the individual or of another natural person, where the individual is physically or legally incapable of giving consent
- Processing is necessary for the establishment, exercise or defence of legal claims
- Processing is necessary for the Purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

5.0 CONSENT

5.1 Where a need exists to request and receive consent of an individual prior to the collection, use or disclosure of personal data, the school is committed to seeking such consent. In all cases consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's wishes. The school is therefore committed to obtaining consent in the following manner:

- consent is presented in a manner clearly distinguishable from other matters
- the request is made in an intelligible and easily accessible form using plain language
- is freely given (i.e. not based on the need to conduct another processing activity)
- the date, method, validity and content of the consent is documented
- a simple method is provided for the data subject to be able to withdraw consent at any time

5.2 Once consent is withdrawn by the data subject, the school will cease processing data for the specified purpose without undue delay.

5.3 If the school wishes to offer information Society Services (ISS) to pupils it will gain parental consent for any pupil below the age of 13.

6.0 ACCOUNTABILITY AND GOVERNANCE

Data Protection Officer (DPO)

6.1 Under the GDPR it is mandatory for Public Sector Bodies (as defined by the FOIA) to designate a Data Protection Officer (DPO). The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for supervisory authorities

6.2 For any queries relating to managing data, in the first instance, please contact Wendy Bridson, Governance Manager on 01254 790026 or wbridson@ept-uk.com.

6.3 The contact details for the Trust's designated DPO are as follows:

- Lee Gardiner, Data Protection Officer, Blackburn with Darwen Borough Council, IT Department, 4th Floor, Town Hall, King William Street, Blackburn, BB1 7DY or by email at Schools.IG@blackburn.gov.uk.

Register of Processing Activities (RoPA)

6.4 The Trust is required to maintain records of activities related to higher risk processing of personal data. The Trust can confirm it maintains a Register of Processing Activities and this is held by the school office in conjunction with the DPO. All members of staff are required to notify the relevant persons before they embark on any new processing activities, so they can be adequately recorded on the RoPA.

Workforce Training

6.5 The Trust is committed to providing data protection training to all staff as part of their induction process and will issue regular refresh training throughout the course of their employment or in the event of any changes in data protection law. The school will retain a record of this training programme and this will be made available to the supervisory authority on request.

Staff for the purpose of this policy includes all staff including student teachers on training placements and these staff would be required to comply with all school policies relating to their appropriate use of personal information.

Data Protection Impact Assessments (DPIA's)

6.6 Data protection impact assessments (DPIAs) are a tool which can help the school identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

6.7 The school will complete DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. Therefore, staff must consult their DPO before they embark on any new processing that could be regarded as being high risk to individuals' interests. If required, the DPO will assist members of staff completing the school's DPIA template.

Contracts

6.8 Whenever a controller uses a processor, it needs to have a written contract in place. This is important so that both parties understand their responsibilities and liabilities. The school contracts should include the following compulsory details in its contracts:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.
- (Please note this is not an exhaustive list, complete lists of compulsory details should be taken into consideration and can be found at: (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/)

7.0 INDIVIDUAL RIGHTS

Right to be informed

7.1 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. We call this 'privacy information' and the school will issue privacy notices in relation to pupil data, workforce data and governor data. The school will endeavour to issue these notices on induction and also make them available on the school's website throughout the data subject's school life.

Right of Access

7.2 Individuals have the right to access their personal data (commonly known as subject access) and supplementary information about the processing of their data. The right of access allows individuals to be aware of and verify the lawfulness of the processing of their personal data. The information that can be requested 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
- 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

7.3 'Subject access' requests can be made to the Trust's Governance Manager by telephone on 01254 790026 or by email to wbridson@ept-uk.com, and must contain the name of the data subject, a correspondence address and a description of the information requested. The information will be sent without delay and at the latest within one calendar month of receipt of the request. The school will not apply a fee to requests unless the request is manifestly unfounded or excessive. The school will take reasonable steps to verify the identification of the applicant and if the applicant wishes to request a review of the school's decision, the process for doing so will be clearly outlined in the response issued.

Individual rights

7.4 The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

7.5 The school will carefully consider any requests under these rights and requests can be made in writing to the school's DPO.

7.6 Further information relating to these rights can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)

8.0 DATA SECURITY

8.1 Principle F states data should be processed in a manner that ensures appropriate security of the personal data. This means the school must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. Particular attention will be paid to the need for security of sensitive personal data.

8.2 Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data. Staff should carefully consider whether they need to take any manual data offsite before doing so and record instances where any 'special categories of data' is taken offsite. The following measures must be taken by staff in relation to electronic data:

- portable electronic devices, such as laptops, ipads and hard drives that contain personal data are stored in a locked cupboard or draw
- encryption software is used to protect all portable devices and removable media that contain personal data, such as laptops and USB devices
- passwords must meet appropriate security standards, be changed at regular intervals and must not be divulged to any other persons
- where personal data is shared with a third party, staff should carry out due diligence and ensure the data is sent in a secure manner or appropriate measures are taken to mitigate the risk of individuals being identified
- when sending personal data to a third party, staff must carefully check the recipient and their contact details
- where personal devices are used to access organisational email accounts, staff should ensure appropriate passwords are applied to the device and they access the accounts by the recommended means i.e. Office 365 users should use the Office 365 application rather than syncing to phone
- staff should not open links when emails are received from unknown recipients or the emails appear suspicious
- personal data must be stored in a secure and safe manner, with careful consideration made to who can access the data

9.0 BREACH REPORTING

9.1 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Where feasible, the school must do this within 72 hours of becoming aware of the breach, it is therefore essential that **all members of staff make the relevant persons aware of any potential breaches of data protection without undue delay.** This includes all losses, thefts or inadvertent disclosures of personal data. It also includes the loss or theft of any device that holds personal data. The relevant persons at the Trust will then follow the breach procedure outlined in Appendix A in conjunction with the DPO.

9.2 The Trust and the DPO will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Trust and the

DPO will follow the relevant procedure based on the criticality and quantity of the personal data involved. For significant personal data breaches, the Trust will carefully consider whether it is required to notify the Information Commissioner and the data subjects affected.

10.0 DATA RETENTION

10.1 Principle F states data must be 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. Data will only be retained for the specified period outlined in the records management schedule that the school has adopted and will be destroyed in a secure manner thereafter. A copy of the records management schedule is available on request from the Trust.

11.0 DATA ACCURACY AND LIMITATION

11.1 The school will issue regular reminders to staff and parents to ensure that personal data held is up to date and accurate. Any inaccuracies discovered should be rectified and if the inaccurate information has been disclosed to a third party; the recipients will be informed of the corrected data.

11.2 The school will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals in the school's privacy notices. 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 to do so in their jobs.

12.0 INFORMATION REQUESTS

12.1 Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. The school will adhere with 'subject access' requests as outlined in Section 7.2 of this policy.

12.2 Personal data will only be disclosed to third party organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given e.g. examination boards.

12.3 Requests for personal data by the Police or other bodies with law enforcement powers (e.g. HMRC), will usually only be considered when accompanied by a data protection form such as a 'Lancashire Constabulary DP1'. This form typically contains details of the applicant, the purpose of the request and the section of the legislation the information is being requested under. This will allow the DPO to make an informed decision as to whether the request is proportionate for the purposes requested, against the rights of the data subject

12.4 If requests are received from parents/carers for the names of pupils in their class (e.g. for Christmas card or birthday invites), only first names will usually be released, however the school reserves the right to refuse any request in its entirety.

13.0 APPENDIX A – BREACH REPORTING PROCEDURE

In the event of a data breach, including a potential breach, the staff member or data processor must immediately notify the Trust's Governance Manager on telephone 01254 790026 or by email at wbridson@ept-uk.com. The reporting member of staff will complete Sections 1-3 of the 'Personal Data Breach Form' before submitting it to the Governance Manager.

The Trust's Governance Manager will liaise with the DPO, who will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully lost, stolen, destroyed, altered or disclosed. The DPO will take the following steps:

- Make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary
- Assess the potential consequences, based on how serious they are, and how likely they are to happen
- Notify the Headteacher and Trust if felt appropriate
- Decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material. If it's likely that there will be a risk to people's rights and freedoms, the DPO will advise the Headteacher that they must notify the ICO

The DPO will document the decision (either way) in Section 7 of the 'Personal Data Breach Form', in case it is challenged at a later date by the ICO or an individual affected by the breach.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach
- the name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

Notify the data subject if the breach is likely to result in a high risk to their rights and freedoms.

Document each breach, irrespective of whether it is reported to the ICO on the 'Personal Data Breach Register'.

The Trust, DPO and Headteacher will discuss each breach to review what happened and how recurrence can be prevented and also share good practice.