Data Protection Policy (GDPR and DPA 2018)

Essex Educare Ltd.

Policy Ref: EE/DPP/001
Version: 1.0
Date Approved: 6th April 2024
Review Date: 6th April 2025
Statutory Basis: General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018)

1. Introduction and Scope

1.1 Purpose

This policy sets out the commitment of Essex Educare Ltd. ("the Company") to protect the privacy and security of personal data collected from students, parents/carers, staff, and other stakeholders. As a data controller, the Company is legally required to comply with the Data Protection Act 2018 and the GDPR.

1.2 Data Protection Officer (DPO)

The Company has appointed a Data Protection Officer (DPO) to oversee compliance with this policy and related legislation.

DPO Contact:

- **Name:** Tashik Uzzaman
- **Role:** Head of Compliance
- **Email:** tashik@eeducare.org.uk

1.3 Scope

This policy applies to all personal data held by the Company, regardless of format (electronic or physical), and to all employees, contractors, volunteers, and Governors/Directors.

2. The Data Protection Principles (GDPR Article 5)

Essex Educare Ltd. is committed to complying with the six fundamental principles of data protection when handling personal data.

Shutterstock

Explore

These principles require that personal data shall be:

Principle	**Commitment by Essex Educare Ltd.**
1. Lawfulness, Fairness, and Transparency	Processed lawfully, fairly, and in a transparent manner. This includes providing clear Privacy Notices to all data

	subjects (e.g., parents, students, staff).
2. Purpose Limitation	Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data Minimisation	Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. We will not collect excessive data.
4. Accuracy	Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
5. Storage Limitation	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 (see Section 5 on Retention).
6. Integrity and Confidentiality	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. Lawful Basis for Processing

The Company will ensure that all processing of personal data has a clear lawful basis, which, in an educational setting, typically falls under one of the following:

- **Legal Obligation:** Necessary for compliance with a legal obligation (e.g., providing data to the Department for Education or HMRC).
- **Public Task:** Necessary for the performance of a task carried out in the public interest or in the exercise of official authority (the core function of providing education).
- **Contract:** Necessary for the performance of a contract with the data subject (e.g., an employment contract with a staff member or service agreement with a parent).

- **Legitimate Interests:** Necessary for the legitimate interests of the Company or a third party, provided these interests are not overridden by the rights and freedoms of the data subject (e.g., using CCTV for security).
- **Consent:** Explicit and freely given consent, typically used for non-essential processing, such as promotional photography or optional newsletters.

Note on Special Category Data (Sensitive Data): Processing of special category data (e.g., health, religious beliefs) requires both a lawful basis *and* an additional condition for processing, such as where it is necessary for the purposes of preventative or occupational medicine (staff/student welfare).

4. Individual Rights of Data Subjects

The Company respects the rights of individuals concerning their data and will handle all requests relating to these rights in accordance with the GDPR:

Right	Company Obligation
Right to be Informed	Provide transparent information about processing activities via clear Privacy Notices.
Right of Access (SAR)	Respond to Subject Access Requests (SARs) within one month (30 calendar days). Extensions may apply for complex cases.
Right to Rectification	Correct inaccurate or incomplete personal data without undue delay upon request.
Right to Erasure ('Right to be Forgotten')	Erase personal data where there is no compelling reason for its continued processing, subject to statutory retention periods and legal exceptions.
Right to Restrict Processing	Temporarily cease processing data in specific circumstances (e.g., while accuracy is being verified).
Right to Data Portability	Provide personal data in a structured, commonly used, and machine-readable format upon request (primarily relevant to data processed by consent or contract).

Right to Object	Cease processing data based on legitimate interests or public tasks if the individual can demonstrate compelling grounds, unless the Company can demonstrate overriding legal grounds.

5. Data Security and Breach Procedure

5.1 Security Measures

The Company maintains robust technical and organisational security measures to protect data from accidental or deliberate threats. These measures include:

- Secure password policies and multi-factor authentication.
- Encryption of sensitive data both in transit and at rest.
- Regular security audits and updates to software.
- Physical security controls for paper records and IT infrastructure.

5.2 Data Breach Management

A personal data breach is a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Procedure:

1. **Detection and Containment:** The staff member detecting the breach must immediately inform the DPO. The DPO will take steps to contain the breach (e.g., isolate the affected system).
2. **Risk Assessment:** The DPO will assess the severity and potential consequences of the breach for the data subjects.
3. **Notification (ICO):** If the breach is likely to result in a risk to the rights and freedoms of individuals, the DPO will notify the Information Commissioner's Office (ICO) **without undue delay, and no later than 72 hours** after becoming aware of it.
4. **Notification (Data Subjects):** If the breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will notify the affected data subjects directly.

6. Data Retention and Disposal

Personal data will be kept for no longer than is necessary for the purposes for which it was collected. The Company will maintain a detailed **Data Retention Schedule** which outlines the statutory and best practice retention periods for various categories of data (e.g., student records, financial information, HR files).

Data destruction will be carried out securely, ensuring that it is permanently irretrievable. This

includes:

- Shredding or incineration of physical documents.
- Secure deletion or physical destruction of electronic storage media.