Date Written: 1st September 2025
Approved by: Directors & Managers

Review Date: September 2027
Signed by: H. Legenby

1st Step Pre-school Ltd: Confidentiality & Data Protection Policy

Our Commitment

1st Step Pre-school Ltd is committed to protecting the privacy of children, families, staff and others, in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Statutory Framework for the Early Years Foundation Stage (EYFS 2025), including section 3.92 on record keeping.
This policy applies to all personal data we hold, whether paper or electronic, and outlines how we collect, use, store, retain, and dispose of information lawfully and securely.

Scope

This policy applies to all:

- Staff and management
- Volunteers, students, and apprentices
- Third parties who handle, store, or process data on behalf of the pre-school

Definitions

- Personal data – information that can identify an individual (e.g., name, date of birth, contact details).
- Special category data – sensitive data (e.g., health, ethnicity, religion, safeguarding information).
- Processing – anything done to personal data, including collection, storage, use, sharing, or disposal.
- Data Controller – the organisation that decides how and why personal data is used 1st Step Pre-school Ltd.
- Data Breach – accidental or unlawful loss, alteration, unauthorised access, or disclosure of personal data.

Roles & Responsibilities

- Data Controller: 1st Step Pre-school Ltd (registered with the ICO – registration number ZB394531).
- Data Protection Lead/DPO: Business Manager, Samantha Martin. Responsible for policy implementation, compliance monitoring, and first point of contact for data queries.
- All staff: Responsible for following this policy, handling data securely, and reporting breaches immediately.

Principles of Data Protection

We are committed to the seven GDPR principles:

1. Lawfulness, fairness & transparency
2. Purpose limitation – used only for legitimate purposes
3. Data minimisation – only what is necessary
4. Accuracy – kept up to date
5. Storage limitation – not kept longer than necessary
6. Integrity & confidentiality – secure at all times
7. Accountability – we can demonstrate compliance

Confidentiality Commitments

- Parents/carers may access their own child's records, but not information about other children.
- Staff do not discuss children, families, or staff matters outside the professional context.
- Information is shared only on a need-to-know basis, and only with consent, unless safeguarding overrides apply.
- Personnel matters remain confidential to those directly involved.
- A private space is available for confidential discussions.
- Staff, volunteers, and students must sign a confidentiality agreement during induction.
- Breaches of confidentiality may result in disciplinary action or suspension of a student's place.

Lawful Basis for Processing Data

- Our lawful basis for processing most personal data is legal obligation under the EYFS and other statutory requirements.
- For optional data uses (e.g., photos for displays or marketing), we require explicit consent.
- Consent is always opt-in and may be withdrawn at any time.

Data We Collect & Use

We collect, hold, and share two types of records:
Developmental Records:

- Observations, photographs, and assessments (e.g., Two-Year Progress Check, Tapestry).
    - Shared with parents regularly to support learning.

Personal Records:

- Registration details, contracts, and funding information.
- Emergency contacts, health and medical needs.
- Safeguarding and child protection records.
- SEND and EHCP information.
- Accident, incident, and medication records.
- Correspondence and reports with outside professionals.

We use this data to:

- Support learning and development
- Safeguard children
- Comply with legislation and funding requirements
- Assess and improve our services

Record Retention & Disposal

Records are retained in line with EYFS 2025 and statutory requirements:

Type of Record	**Retention Period**
Child registration forms	3 years after child leaves
Attendance registers	3 years after child leaves
Accident/incident	3 years after child leaves
Child protection files	Until child is 21*
SEND records	Until child is 25*
Medication forms	3 years after child leaves
Complaints records	3 years
Local Authority funding documents	7 years + current year
Employment/payroll records	6 years
DBS disclosures	No longer than 6 months
Non-statutory records (e.g. Tapestry profile)	Transferred to parents on leaving
Photos & marketing images	Until no longer required or consent withdrawn

**Unit the child is 75 for Looked After Children*

All paper files are kept in locked cabinets. Electronic records are password-protected and access-controlled. Records are securely shredded or permanently deleted once no longer required.

Data Sharing

We share information only when necessary, securely, and in line with the law.
We routinely share data with:

- Schools that children move on to
- Local Authority (e.g. funding, Early Years Census)
- Department for Education (DfE)
- Safeguarding partners (when required)
- We may also share data with HMRC, law enforcement, or emergency services if legally required.

Individual Rights

Individuals have the following rights regarding their personal data:

- To be informed about how data is used
- To access their data (Subject Access Request)
- To request rectification or erasure
- To restrict or object to processing
- To request portability of their data
- To withdraw consent at any time
- To be informed of a data breach where relevant

Subject Access Requests (SARs):

- Must be made in writing (email or letter) to the Data Protection Lead.
- Nursery may request proof of ID.
- Requests will be answered within one calendar month (or three months if complex).
- For children under 12, parents may usually act on their behalf unless the child is deemed mature enough to understand their rights.

Data Breaches

If a data breach occurs:

- It will be reported immediately to the Central Office.
- Serious breaches will be reported to the ICO within 72 hours.
- Affected individuals will be informed if necessary.
- All breaches will be logged, investigated, and reviewed.

Staff Training & Responsibilities

- All staff receive training on confidentiality and data protection.
- Staff are personally responsible for following this policy.
- Staff may be personally liable under the Data Protection Act if they misuse data.
- Serious breaches may result in disciplinary action, up to dismissal.

Legal Framework

This policy is based on:

- UK GDPR (2018)
- Data Protection Act (2018)
- Freedom of Information Act (2000)
- Human Rights Act (1998)
- Children Act (2004)
- DBS Code of Practice
- EYFS Statutory Framework (2025), section 3.92