



My Little Explorers

Data Protection Policy

Statement of Intent

My Little Explorers is committed to safeguarding and promoting the welfare of children and expects all staff, students and volunteers to share this commitment. We recognise that the lawful, secure and respectful handling of personal data is fundamental to protecting children, supporting families and meeting our statutory responsibilities.

This policy sets out how personal data is collected, stored, shared, retained and disposed of in accordance with the Early Years Foundation Stage (EYFS), UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Ofsted requirements, and in alignment with our Confidentiality Policy and Safeguarding and Child Protection Policy.

Aims

We aim to ensure that all personal data held by the setting is:

- Collected lawfully, fairly and transparently
- Used only for specified and legitimate purposes
- Accurate, relevant and kept up to date
- Stored securely and protected from unauthorised access
- Shared appropriately and proportionately
- Retained only for as long as necessary
- Disposed of safely and confidentially

Legal Framework

This policy has regard to the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Early Years Foundation Stage (EYFS) Statutory Framework

- Working Together to Safeguard Children
- Human Rights Act 1998
- Limitation Act 1980
- Employers' Liability (Compulsory Insurance) Regulations 1998
- Disclosure and Barring Service (DBS) guidance

Relationship to Other Policies

This policy must be read alongside:

- Confidentiality Policy
- Safeguarding and Child Protection Policy
- Complaints Policy

Where there is any conflict between data protection, confidentiality and safeguarding requirements, the welfare of the child is paramount and safeguarding takes precedence.

Data Controller and Registration

My Little Explorers is the Data Controller for all personal data held within the setting.

ICO Registration Number: ZB997301

Where third-party providers are used (e.g. digital learning journals), we ensure that appropriate data processing agreements are in place and that providers comply with UK GDPR.

GDPR Principles

We process personal data in line with the GDPR principles, ensuring that data is:

1. Processed lawfully, fairly and transparently
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up to date
5. Retained only for as long as necessary
6. Processed securely

7. Protected against unauthorised or unlawful processing, loss or damage
8. Not transferred to non-compliant organisations or jurisdictions

Lawful Basis for Processing

Personal data is processed only where a lawful basis applies, including:

- Legal obligation (e.g. EYFS record-keeping, safeguarding duties)
- Contract (e.g. parent agreements, funding claims)
- Consent (e.g. photographs, marketing materials)
- Vital interests (e.g. medical emergencies)
- Public task (e.g. safeguarding responsibilities)
- Legitimate interests, where appropriate and proportionate

Consent may be withdrawn at any time, except where processing is required by law or safeguarding duty.

Confidentiality and Information Sharing

- All personal data is treated as confidential and shared only on a need-to-know basis, in line with our Confidentiality Policy.
- Staff must not discuss personal or sensitive information outside the setting or with unauthorised individuals.
- Information may be shared internally where necessary to support:
 - Safeguarding
 - Children's learning and development
 - Individual care and support needs

Safeguarding Override

While we respect confidentiality and data protection, the welfare of the child is paramount.

Personal data may be shared without parental consent where:

- There is a safeguarding concern

- A child is at risk of harm
- Disclosure is required by law

Staff must not promise confidentiality to a child or family where safeguarding concerns are present and must follow reporting procedures without delay.

All information sharing decisions are recorded in line with statutory guidance and our Safeguarding Policy.

Individual Rights

Parents, carers and staff have the right to:

- Be informed about how their data is used
- Access personal data held about them or their child
- Request correction of inaccurate information
- Request erasure where lawful
- Restrict or object to processing where applicable

Requests are managed in line with our Confidentiality Policy and statutory timeframes.

Data Security

- Paper records are stored in locked cabinets within secure areas.
- Digital records are:
 - Password-protected
 - Access-restricted
 - Stored on GDPR-compliant systems

All staff receive training on data protection, confidentiality and safeguarding as part of induction and ongoing supervision.

Data Breaches

Any actual or suspected data breach:

- Is reported immediately to the Setting Manager

- Is investigated and recorded
- Is reported to the ICO where legally required
- Is reviewed to minimise future risk

Record Retention

General Principles

Records are retained only for as long as necessary to meet legal, safeguarding, regulatory and operational requirements. Where safeguarding concerns exist, records will be retained beyond standard retention periods in line with statutory safeguarding guidance and advice from the Local Authority or other relevant agencies.

Key Retention Periods (Summary)

Record Type	Retention Period
Child personal details	Closure of setting + 50 years
Parent contact details	With child record or destroyed on leaving
Attendance registers	Minimum 3 years, or longer where safeguarding applies
Accident & incident records (child)	Child's date of birth + 25 years
Medication records	Child's date of birth + 25 years
Safeguarding / child protection records	Until the child reaches 25 years of age or longer if advised
Complaints relating to EYFS	Minimum 3 years
Staff personnel files	Employment end + 6 years
Allegations against staff	Retirement age or 10 years (whichever is longer)

Full retention schedules are maintained internally and reviewed regularly.

Disposal of Records

- Paper records are cross-shredded or disposed of using a confidential waste service
- Digital records are permanently deleted
- Disposal is logged using a Record Disposal Schedule

Responsibilities

- The Setting Manager is responsible for overseeing compliance with this policy.
- All staff are responsible for:
 - Handling data securely
 - Maintaining confidentiality
 - Following safeguarding procedures
 - Reporting concerns or breaches immediately

This policy was reviewed on	This policy was reviewed by	Date for review
15/09/2025	Sam Victoria	September 2026