Innsworth Preschool Data Protection and Confidentiality Policy
Last Updated: 1st January 2026

1. Purpose and Commitment

1.1 Overview: This policy outlines how Innsworth Preschool upholds the protection of all personal and sensitive data as a fundamental part of our safeguarding duty.

1.2 Commitment: We are committed to handling all information professionally, lawfully, and securely in a manner that protects the privacy of our children, families, and staff.

1.3 Data Controller: Innsworth Preschool is the Data Controller for the purposes of Data Protection legislation.

- **Contact:** The Business Manager
- **Address: I**nnsworth Preschool, Luke Lane, **I**nnsworth, Gloucester, GL3 1HJ
- **Email:** data@innsworthpreschool.co.uk

2. Statutory Framework

2.1 Compliance: This policy is underpinned by and ensures compliance with the following legislation:

- The UK General Data Protection Regulation (UK GDPR).
- The Data Protection Act 2018 (DPA 2018).
- The Statutory Framework for the Early Years Foundation Stage (EYFS).
- The Children Acts 1989 & 2004.
- Working Together to Safeguard Children.

2.2 EYFS Requirements: In accordance with the EYFS:

- We maintain records and share relevant information with parents, other professionals, the police, social services, and Ofsted as appropriate.
- Confidential records are kept secure and accessible only on a "need to know" basis.
- Parents are given access to records about their child, provided no DPA exemption applies (e.g. risk of harm).
- Children's records are retained for a reasonable period after they have left the setting.

3. Data Protection Principles & Lawful Basis

3.1 Principles: We adhere to the key principles of the UK GDPR, ensuring that all personal data is processed lawfully, fairly, and transparently.

3.2 Lawful Basis for Processing (Article 6): We process personal data under specific lawful bases:

- **Contract:** To provide the childcare service (e.g. attendance, billing).
- **Legal Obligation:** To meet statutory duties (e.g. safeguarding, Ofsted reporting, funding claims).
- **Vital Interests:** To protect a child's life (e.g. emergency medical data).
- **Legitimate Interests:** For legitimate business purposes (e.g. CCTV security, administration).
- **Consent:** For optional, non-essential processing (e.g. marketing photos, social media publicity).

3.3 Special Category Data (Article 9): We process sensitive data (health, ethnicity, safeguarding) under stricter conditions. We identify the relevant Article 9 condition and, where required, the DPA 2018 Schedule 1 condition before processing:

- **Health/Medical Data:** Processed for the provision of health or social care (Article 9(2)(h)) to ensure safe daily care.
- **Safeguarding:** Processed for reasons of substantial public interest (Article 9(2)(g)) and the safeguarding of children (DPA 2018 Schedule 1, Part 2).
- **Legal Claims:** Processed for the establishment, exercise, or defence of legal claims (Article 9(2)(f)) (e.g. accident records for insurance).
- **Policy Document:** Where we rely on a DPA 2018 Schedule 1 condition, we maintain an Appropriate Policy Document.

4. Information Sharing

4.1 Safeguarding Primacy: Our primary responsibility is safeguarding.

- **Statutory Duty:** We share information with agencies such as Children's Social Care, the Police, or the LADO where there is a concern a child is at risk of harm.
- **Consent Override:** Parental consent is NOT required for safeguarding disclosures if seeking it would place a child at increased risk or prejudice a police investigation.

4.2 Method: We share only the minimum necessary information via secure, approved channels (e.g. encrypted email or secure portal). Sharing sensitive data via informal parent WhatsApp groups is prohibited.

5. Processors & CCTV

5.1 Processors: We use carefully selected third-party processors (e.g. Tapestry). We conduct due diligence and hold binding Data Processing Agreements ensuring data security, location of storage, sub-processor controls, and deletion on termination.

5.2 CCTV: If CCTV is used:

- **Purpose:** For security and the prevention/detection of crime.
- **Governance:** We display clear signage, restrict access, and retain footage for [Insert Period, e.g. 30 days].
- **Assessment:** We maintain a Legitimate Interests Assessment (and DPIA if high risk) for the system.

6. Your Rights (Subject Access Requests)

6.1 Right of Access: Parents and staff may request a copy of the data we hold about them (Subject Access Request).

- **Process:** Requests can be verbal or written. We may request ID to verify identity.
- **Timeline:** We respond within one calendar month (extendable by two months for complex requests).
- **Redaction:** We will redact third-party data (identifying other children, families, or staff) unless consent is obtained or it is reasonable to disclose without it.

6.2 Right to Erasure: You may request deletion, but this is NOT absolute. We will not erase data where continued retention is necessary for safeguarding, statutory compliance, or the defence of legal claims.

6.3 Complaints: If you are unhappy with how we handle your data, please contact the Business Manager first. You have the right to lodge a complaint with the Information Commissioner's Office (ICO).

7. Data Retention Schedule

7.1 Policy: We retain records for a reasonable period to meet legal and operational needs.

7.2 Safeguarding / Child Protection:

- **Retention:** Until child is 25 (or per Local Authority requirement).
- **Rationale:** Statutory inquiry / abuse claims.

7.3 Accident / Incident Records:

- **Retention:** Until child reaches 21 years and 3 months.
- **Rationale:** Limitation Act 1980 (Personal Injury claims).

7.4 Attendance Registers:

- **Retention:** 3 years after the last entry.
- **Rationale:** Statutory Framework EYFS / Audit.

7.5 Funding / Financial Records:

- **Retention:** 6 years + current year.
- **Rationale:** HMRC / Company law requirements.

7.6 Staff HR Files:

- **Retention:** 6 years after employment ends.
- **Rationale:** Employment law / contract claims.

7.7 Children's Learning Journals:

- **Retention:** Until child leaves (transferred to parent/school).
- **Rationale:** Educational transition.

7.8 Disposal: Records are securely destroyed (shredded or digitally wiped) once the retention period expires.

8. Data Security & Smart Devices

8.1 Mobile Phones & Smart Devices: To prevent data capture and distraction:

- **Designated Areas:** Personal mobile phones and camera-enabled smartwatches are strictly prohibited in designated child-contact areas (including playrooms, nappy changing areas, toilets, sleeping rooms, and outdoor play zones).
- **Storage:** Staff, visitors, and contractors must store devices in the office or designated lockers. Exceptions (e.g. for medical monitoring apps) must be authorised by the Manager in writing.

- **Enforcement:** Repeated refusal to comply is a safeguarding concern and may result in removal from the site.

9. Parent Responsibilities & Social Media

9.1 Accuracy: Parents must ensure contact details are accurate and up to date.

9.2 Social Media:

- **Personal Use:** Parents may photograph *their own* children at specific events for personal use.
- **Prohibition:** You must NOT post images or videos containing *other people's children* on public social media or share them in public groups without permission.
- **Breach: I**f a parent refuses to remove content featuring other children, we will treat this as a safeguarding/privacy breach. This may result in restrictions on photography at future events or conduct proceedings.

10. Staff Responsibilities

10.1 Confidentiality: Staff must not discuss sensitive child or family information in public areas. Disclosing confidential information verbally is serious misconduct.

11. Data Breach Procedures

11.1 Immediate Action: We maintain an internal breach log. In the event of a suspected breach, we assess the risk to individuals' rights and freedoms.

11.2 Reporting:

- **ICO: I**f the breach is reportable (high risk), we notify the ICO within 72 hours.
- **Individuals:** We notify affected individuals without undue delay if there is a high risk to their rights.
- **Escalation:** We maintain an out-of-hours contact to ensure we meet reporting deadlines.

12. Freedom of Information

12.1 Status: As a private provider, we are not a public authority for the purposes of the Freedom of Information Act 2000 (FOIA). We respond to requests under Data Protection legislation and our contractual terms, unless acting on behalf of a public authority in a specific capacity that engages FOIA.

13. Monitoring and Review

13.1 Review: This policy is reviewed annually.