# Little Acorns Montessori

Ascot | Bracknell | Crowthorne

# CONFIDENTIALITY POLICY

## Document Control

| | |
|---|---|
| **Version** | 1.0 |
| **Date Adopted** | June 2026 |
| **Review Date** | June 2027 |
| **Author** | Jonathan Duffy - Director |
| **ICO Registration Number** | ZA161231 (registered since 26 January 2016) |

## 1. Policy Statement

Little Acorns Montessori is committed to safeguarding the privacy and dignity of every child in our care, together with their families and all members of staff. We recognise that information shared with us is shared in trust, and we treat all personal data with the utmost care and discretion.

This policy sets out how we collect, store, use, share and dispose of confidential information. It applies to all settings operated by Little Acorns Montessori (Ascot, Bracknell and Crowthorne), all employees (permanent, temporary, bank and volunteer), students on placement, and contractors acting on our behalf.

Confidentiality is never a barrier to safeguarding. Where there is a conflict between maintaining confidentiality and protecting a child from harm, the welfare of the child will always take priority.

## 2. Statutory Framework and Legal Basis

This policy fulfils our legal and regulatory obligations under the following legislation and guidance:

| Legislation / Guidance | Relevance to this Policy |
|---|---|
| EYFS Statutory Framework 2025 (effective 1 Sep 2025)Requirements 3.94 GP (Privacy) | Providers must ensure all staff understand the need to protect children's privacy and the legal requirements for handling information about children. |
| EYFS 2025 – Information & Records (Reqs 3.84–3.93 GP) | Records must be easily accessible and available. Confidential records about staff and children must be held securely and only accessed by those with a right or professional need to see them. |
| UK General Data Protection Regulation (UK GDPR) | Governs all processing of personal data. Individuals hold rights of access, rectification and erasure. Data must be held lawfully, fairly and transparently. |
| Data Protection Act 2018 | Supplements UK GDPR. Sets out exemptions and enforcement. Requires annual registration with the ICO. |

| | |
|---|---|
| Working Together to Safeguard Children 2026 | Sets out multi-agency information-sharing requirements. Clarifies when parental consent is not required before sharing information. Includes a dedicated section on partnership working with early education and childcare providers. Reinforces that the Data Protection Act 2018 and UK GDPR do not prevent information sharing to keep children safe. |
| Children Act 1989 & 2004 | Establishes the paramount principle that the welfare of the child is the overriding consideration. |
| Human Rights Act 1998 (Article 8) | Confers the right to respect for private and family life. Any interference must be lawful, necessary and proportionate. |
| Freedom of Information Act 2000 | May apply where Little Acorns Montessori receives public funding. Advice to be sought from the relevant local authority if in doubt. |
| DfE Information Sharing Advice for Safeguarding Practitioners 2024 | Non-statutory guidance on when and how to share information lawfully to support safeguarding decisions. |
| Ofsted Education Inspection Framework 2025 (in effect from 10 November 2025) | Inspectors review whether policies and procedures protect children and comply with statutory requirements. The 2025 framework introduces a multi-area report card system in place of single-word grades. Safeguarding remains a separate binary judgement. Settings should ensure that confidentiality policies and practices are evidenced in everyday provision, not solely in paperwork. |

## 3. Scope

This policy applies to all confidential information held by Little Acorns Montessori, including but not limited to:

- Personal and sensitive data relating to children (including developmental records, health information, SEND support plans, incident and accident records, and child protection files).
- Personal data relating to parents and carers (contact details, financial information, parenting orders, court orders).
- Personnel records for all staff, volunteers and students on placement.
- Commercially sensitive or operational information about the nursery.
- Information shared verbally, in writing, electronically or through any other medium.

## 4. Roles and Responsibilities

| Campus | Data Protection Officer | Data Controller |
|---|---|---|
| Bracknell | Agata Payne | Jonathan Duffy |
| Ascot | Elaine Eastham | Jonathan Duffy |
| Crowthorne | Emma Gray | Jonathan Duffy |

## 4.1 Nursery Manager

- Must ensure this policy is implemented, reviewed annually and communicated to all staff.
- Must ensure the setting is registered with the ICO and that the registration is renewed each year.
- Must ensure that all contracts of employment and volunteer agreements include a confidentiality clause.
- Must oversee the secure storage of all confidential physical and electronic records.
- Must appoint a DSL and Deputy DSL and ensure they receive training in line with EYFS 2025 Annex C requirements (mandatory training every two years with annual refreshers).

## 4.2 Designated Safeguarding Lead (DSL)

- Must act as the primary point of contact for all matters involving confidential safeguarding information.
- Must ensure that information relating to child protection concerns is shared with the relevant statutory agencies (children's social care, police) without delay when there is risk to a child.
- Must keep confidential records relating to safeguarding concerns in a separate, secure file, distinct from the child's general development file.
- Must determine, on a case-by-case basis, whether parental consent is required before sharing information with external agencies, following the DfE Information Sharing Advice 2024.
- Must record the rationale for every decision to share or not to share information.

## 4.3 Deputy DSL

- Should act in the absence of the DSL with full authority in relation to confidentiality and safeguarding decisions.
- Must be trained to the same standard as the DSL.

## 4.4 All Staff, Volunteers and Students

- Must maintain confidentiality at all times, both within and outside the setting.
- Must not discuss information about individual children or families outside the nursery, including on social media platforms.
- Must not access records relating to children or families other than those they have a direct professional need to see.
- Must report any suspected breach of confidentiality to the Nursery Manager or DSL without delay.
- Must complete confidentiality and data protection training at induction and at each refresh required by the Manager.
- Must understand that they cannot agree to keep secrets with a child or parent that would prevent them from reporting a safeguarding concern to the DSL.

## 4.5 Parents and Carers

- Have a right of access to all records held about their own child, subject to any legal restrictions (e.g. where access would place the child at risk).
- Must not be given access to records relating to any other child.
- Should be informed, at the point of enrolment, how their data and their child's data will be stored, used and shared.
- Should understand that information shared with staff about their child may be shared within the team on a need-to-know basis to support that child's welfare and development.
- Should be made aware that the nursery cannot be held responsible if information they voluntarily share with other parents is then passed on.

# 5. Detailed Procedures

## 5.1 Receiving Confidential Information

- When a parent, carer or professional shares confidential information with a member of staff, that member of staff must listen carefully and acknowledge receipt.
- Staff must not promise to keep information confidential if that information relates to the welfare or safety of a child.
- If a parent requests a confidential conversation, staff should direct them to a private area of the setting (away from other adults and children).
- Information received verbally that has a bearing on a child's welfare must be recorded in writing on the same day and passed to the DSL.

## 5.2 Sharing Information Within the Setting

- Information about individual children must only be shared with staff who have a direct professional need to know (e.g. the child's key person, SENCO, DSL).
- Staff must not discuss sensitive information about children or families in communal areas, corridors or in earshot of other families or children.
- Where a child's welfare requires it, relevant information must be shared with the DSL, even where the source asked for confidentiality.
- Staff should not share personal opinions about families with colleagues. Discussions must be professional and factual.

## 5.3 Sharing Information with External Agencies

Working Together to Safeguard Children 2026 and the UK GDPR make clear that data protection law is not a barrier to information sharing where a child's welfare or safety is at risk. Staff should approach information sharing with a presumption in favour of sharing where there is a safeguarding purpose and a lawful basis to do so. Uncertainty should always be resolved in favour of protecting the child.

- Information must ordinarily only be shared with external agencies with the informed consent of the parent or carer.
- Parental consent should NOT be sought before sharing information where doing so could:
  - Place a child or another person at risk of harm.
  - Result in the destruction of evidence or obstruct a police investigation.
  - Result in a serious offence going unreported.
- Where information is shared without consent, this must be recorded in writing, including the rationale for the decision, by the DSL.
- The DSL must follow the procedures of the Local Safeguarding Partners (Bracknell Forest / Slough / Windsor & Maidenhead as appropriate) when making referrals to children's social care.
- All referrals must be confirmed in writing within 24 hours if made verbally by telephone.
- Students on Pre-school Learning Alliance, Level 2, Level 3 or other recognised placement programmes must be briefed on this confidentiality policy before they begin their placement and must sign a confidentiality agreement.

## 5.4 Photographs and Digital Media

- Staff must not take photographs of children on personal devices. Only nursery-owned devices, approved by the Manager, may be used.
- Images of children may only be shared with parents via the nursery's secure, password-protected platform.
- Staff must obtain written parental consent before using images of a child for any purpose, including display within the nursery.
- No images of children may be posted to social media by staff, even where faces are obscured.

### 5.5 Data Breach Procedure

- Any suspected or confirmed breach of confidentiality (including loss of physical records, unauthorised access or inadvertent disclosure) must be reported to the Manager and DSL immediately.
- The Manager must assess whether the breach constitutes a reportable incident under UK GDPR (i.e. likely to result in risk to the rights and freedoms of individuals).
- Where reportable, the Manager must notify the ICO within 72 hours of becoming aware of the breach.
- Affected individuals must be notified without undue delay where there is a high risk to their rights or freedoms.
- All breaches must be recorded in the Nursery's Data Breach Log, regardless of severity.

## 6. Recording and Storage of Confidential Information

### 6.1 Physical Records

- All physical confidential records must be stored in a lockable filing cabinet within the nursery's office, accessible only to the Manager, DSL and authorised staff.
- Child protection files must be stored separately from general development files.
- Records must not be left unattended on desks or in areas accessible to parents, children or unauthorised visitors.
- Confidential documents that are no longer required must be shredded using a cross-cut shredder. They must not be placed in general waste or recycling.

### 6.2 Electronic Records

- Electronic records containing personal data must be stored on password-protected systems, accessible only to authorised staff.
- Where a cloud-based management platform is used (e.g. an early years management system), the Manager must ensure the provider is UK GDPR compliant.
- Staff must not store confidential information on personal devices or personal cloud storage accounts.
- Email containing personal data should be sent via secure means. Staff must not send sensitive personal data to personal email addresses.

### 6.3 Record Retention and Disposal

📋 **Recommended Retention Periods (EYFS 2025 / IRMS Education Records Toolkit / Limitation Act 1980):**

• Child's general development records: Until child's 25th birthday (or 26th if SEND) — if last entry made before child's 17th birthday.

• Accident / incident records (children under 18): Date of birth + 22 years (Limitation Act 1980, s.11 — limitation period suspended until child turns 18).

• Safeguarding / child protection records (referral led to CIN/CP plan or police referral): Until child's 25th birthday. Looked After Children: 75 years.

• Welfare concerns referred for early help (did not escalate to CP plan): 6 years from date referral made. Looked After Children: 75 years.

• Medication administration records: Date of birth + 22 years (Limitation Act 1980, s.11 — personal injury claim period suspended until child turns 18; additional buffer applied).

• Nappy change / personal care / sleep records (daily care diaries): 6 years after child leaves setting as minimum; until child's 25th birthday recommended (records are safeguarding documents under EYFS 2025).

• RIDDOR-reportable incidents (dangerous occurrences, serious injuries): Minimum 3 years from incident date (RIDDOR 1995, statutory); where a child is involved, date of birth + 22 years governs if longer.

• Incidents with a welfare/safeguarding dimension (serious injury, regular medication, severe allergy, serious illness): Until child's 25th birthday. Looked After Children: 75 years.
• Choking incident logs (EYFS 2025 new requirement): Until child's 25th birthday; review logs monthly as required by EYFS 2025.
• SEND files, Education Health and Care Plans, Support Plans: Until child's 25th birthday.
• Photographic/video permissions: 21 years and 6 months from date of permission.
• Complaints (general): Current year + 6 years. If negligence involved: current year + 15 years. If child protection involved: current year + 40 years.
• Staff allegation of a child protection nature: Until staff member's normal retirement age or 10 years from the allegation date, whichever is longer (malicious allegations must be removed from personnel files).
• Staff personnel files and training records: Termination of employment + 7 years.
• Employer liability insurance certificates: Closure of setting + 40 years.
• Staff personnel records: 6 years after employment ends.
• Payroll records: 6 years.
• ICO Registration: Renew annually — lapse is a criminal offence.

⚠ **Always seek advice from your local authority or professional body if uncertain about retention periods.**

- Records must be destroyed securely at the end of the retention period (see Section 6.1 for physical records; electronic records must be permanently deleted and removed from backups where possible).
- A log of records destroyed must be maintained, noting the type of record, date of destruction and method.

## 7. Confidentiality and Safeguarding

Confidentiality must never be used as a reason to withhold information that is relevant to the protection of a child. The following principles apply:

- All staff must understand that the safety and wellbeing of the child overrides the duty of confidentiality.
- Staff must not make promises of secrecy to children or adults. If a child begins to disclose information, staff must explain gently that they may need to share what is said with someone who can help.
- Any disclosure or concern must be reported to the DSL without delay, and recorded using the nursery's Concern Recording Form on the same day.
- The DSL must make all referrals to children's social care in accordance with the Local Safeguarding Partners' procedures for Bracknell Forest, Slough, or Windsor and Maidenhead, as appropriate to the child's home area.
- Staff must not investigate allegations themselves or share information about an allegation more widely than is necessary.
- All staff must be aware of, and able to identify and challenge, racism and discrimination in the context of safeguarding. Leaders are responsible for creating an inclusive culture in which discriminatory practice is actively challenged and in which children's differing backgrounds, experiences and identities are considered in all safeguarding decisions. This reflects the requirements of Working Together to Safeguard Children 2026.

## 8. Training and Awareness

- All new staff must complete induction training that includes the requirements of this policy before working unsupervised with children.
- All staff must undertake data protection and confidentiality refresher training at intervals determined by the Manager, and at minimum every two years.
- The DSL and Deputy DSL must undertake safeguarding training as required by EYFS 2025 Annex C (mandatory training every two years; annual refreshers recommended).

- Training records must be maintained and made available to Ofsted on inspection.
- The Manager should document how staff demonstrate application of their confidentiality training in practice (in line with EYFS 2025 requirements for safeguarding policy content).

## 9. Complaints and Breaches of this Policy

- Any parent, carer or member of staff who believes that confidential information has been mishandled should raise the matter with the Nursery Manager in the first instance.
- If the complaint relates to the Manager, it should be directed to the nursery owner or proprietor.
- All complaints relating to data protection or confidentiality must be investigated promptly and a written response provided within 28 days.
- Where a complaint cannot be resolved internally, the complainant may refer the matter to the Information Commissioner's Office (ico.org.uk).
- Staff who breach this policy may be subject to disciplinary action, up to and including dismissal.

## 10. Policy Review

This policy must be reviewed:

- Annually by the Nursery Manager.
- Following any significant change to relevant legislation or statutory guidance.
- Following any serious breach of confidentiality.
- Following any Ofsted inspection where recommendations are made.

All staff must be notified of any updates to this policy, and a signed acknowledgement must be obtained and retained on their personnel file.

## 11. Related Policies

This policy should be read in conjunction with the following Little Acorns Montessori policies:

- Safeguarding and Child Protection Policy
- Data Protection and Privacy Notice (Children and Families)
- Children's Records Policy
- Staff Code of Conduct
- Whistleblowing Policy
- Staffing and Employment
- E-Safety
- Complaints Policy

## Policy Sign-Off

| Role | Name | Date |
|---|---|---|
| Owner/Director | Jonathan Duffy | June 2026 |

This policy has been written in accordance with the EYFS Statutory Framework 2025 (effective 1 September 2025), UK GDPR, the Data Protection Act 2018, Working Together to Safeguard Children 2026 (published 18 March 2026), the DfE Information Sharing Advice for Safeguarding Practitioners 2024, and the Ofsted Education Inspection Framework 2025 (in effect from 10 November 2025).