Little Acorns Montessori

General Data Protection Regulation (GDPR) Policy

Bracknell | Ascot | Crowthorne

1. Document Control

Field	Details
Policy Title	General Data Protection Regulation (GDPR) Policy
Version	1.0
Date of Issue	June 2026
Next Review Date	June 2027
Author / Owner	Jonathan Duffy
Job Role	Owner/Director
ICO Registration Number	ZA161231 (registered since 26 January 2016)
Applies To	All staff, volunteers, management, and students on placement at Little Acorns Montessori Bracknell, Ascot, and Crowthorne campuses

2. Policy Statement

Little Acorns Montessori Limited is committed to protecting the privacy, dignity, and legal rights of every individual whose personal data we hold. This policy sets out how we collect, use, store, share, and dispose of personal data in full compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy applies to all personal data held about children, parents and carers, staff, volunteers, visitors, and prospective families — whether stored electronically, in paper files, or in any other format.

Little Acorns Montessori Limited is registered with the Information Commissioner's Office (ICO) under registration reference ZA161231.

3. Statutory and Legal Framework

This policy fulfils obligations arising from the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR) — retained in UK law under the European Union (Withdrawal) Act 2018
- Data Protection Act 2018
- Data (Use and Access) Act 2025 (DUAA) — received Royal Assent 19 June 2025; core provisions in force from 5 February 2026 and further provisions from 19 June 2026. This Act amends the UK GDPR and the Data Protection Act 2018 and is now part of the applicable legal framework governing how Little Acorns Montessori Limited processes personal data.
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Human Rights Act 1998
- The Children Act 1989 and 2004 (Every Child Matters)
- Childcare Act 2006

- Statutory Framework for the Early Years Foundation Stage (EYFS) 2024 — in particular:
  - Section 3.69: Providers must maintain records and share information with parents, carers, other professionals, the police, social services, and Ofsted as appropriate
  - Section 3.70–3.73: Requirements relating to staff suitability and information held on children and employees
- Keeping Children Safe in Education (KCSIE) 2025 — referred to as best practice guidance; note that KCSIE is statutory guidance for schools and colleges under the Education Act 2002. As a private early years provider, Little Acorns Montessori Limited's primary statutory safeguarding framework is the EYFS Statutory Framework 2024 and Working Together to Safeguard Children 2023. KCSIE principles are adopted where relevant to early years safeguarding practice and record-keeping.
- Working Together to Safeguard Children 2023
- Information and Records Management Society (IRMS) Retention Schedule for Education 2022
- ICO Guidance on Data Protection in Education

4. Data Protection Principles

In accordance with Article 5 of the UK GDPR, Little Acorns Montessori Limited must ensure that all personal data is:

- Processed lawfully, fairly, and in a transparent manner.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (data minimisation).
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which it is processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.
- Not transferred to a country or territory outside the UK unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.
- Processed in a manner for which the controller is accountable — Little Acorns Montessori Limited must be able to demonstrate compliance with all of the above principles at any time. This is fulfilled through the maintenance of a Record of Processing Activities (ROPA), completion of Data Protection Impact Assessments where required, staff training records, and this policy itself.

Note on Lawful Bases (updated June 2026): The Data (Use and Access) Act 2025 introduced a seventh lawful basis for processing under Article 6 of the UK GDPR: "Recognised Legitimate Interests" (RLI). This applies to a defined set of pre-approved purposes in the public interest — including safeguarding and national security — and does not require a balancing test. Where Little Acorns Montessori Limited relies on this basis, it will be documented in the Record of Processing Activities (ROPA) and reflected in the relevant Privacy Notice. The DPO is responsible for monitoring ICO guidance on RLI as it develops and updating the ROPA accordingly.

5. Roles and Responsibilities

5.1 Designated Data Protection Officer (DPO)

The DPO for each setting must:

- Ensure this policy is implemented, maintained, and reviewed annually.
- Act as the first point of contact for all data protection queries, subject access requests, and breach reporting.
- Liaise with the ICO on compliance matters.
- Deliver or arrange data protection training for all staff.
- Maintain the Record of Processing Activities (ROPA).

5.2 Designated Data Controller — All Campuses

Jonathan Duffy is the Designated Data Controller for all three campuses and is responsible for ensuring the lawful basis for processing all personal data held by Little Acorns Montessori Limited.

5.3 Campus-Level Contacts

Campus	Data Protection Officer	Data Controller
Bracknell	Agata Payne	Jonathan Duffy
Ascot	Rachel Terry	Jonathan Duffy
Crowthorne	Emma Gray	Jonathan Duffy

5.4 All Staff Must:

- Complete data protection training upon induction and annually thereafter.
- Handle all personal data with confidentiality and only access data relevant to their role.
- Never share personal data outside the setting without authorisation from the DPO or Data Controller.
- Report any suspected data breach immediately to the DPO without delay.
- Store paper records securely in locked filing cabinets and never remove them from the setting without authorisation.
- Use password-protected devices at all times; never use personal devices to store setting data.

5.5 Parents and Carers Must:

- Provide accurate personal data at the point of registration and notify the setting promptly of any changes.
- Not share information about other families or children obtained through contact with the setting.

5.6 Data Processors and Article 28 Agreements:

A data processor is any third party that processes personal data on behalf of Little Acorns Montessori Limited. This includes, but is not limited to: Famly; payroll software or bureau; any childcare management system; and any IT support provider with access to systems holding personal data.

Before engaging any data processor, the Data Controller (Jonathan Duffy) must:

- Confirm that the processor provides sufficient guarantees to implement appropriate technical and organisational security measures (Article 28(1));

- Ensure a written Data Processing Agreement (DPA) is in place that meets the requirements of Article 28(3) of the UK GDPR, covering: the subject matter and duration of processing; the nature and purpose of the processing; the type of personal data and categories of data subjects; and the obligations and rights of the controller;
- Ensure that any sub-processors engaged by the processor are subject to equivalent contractual obligations;
- Retain copies of all DPAs and review them periodically or when the nature of the processing changes.

A register of all active data processors and their associated DPAs is maintained by the DPO as part of the Record of Processing Activities (ROPA).

6. Personal Data We Collect and Why

6.1 Children's Data

We collect and process the following data about children in our care, on the lawful basis of legal obligation (EYFS) and legitimate interests:

- Full name, date of birth, birth certificate number, and home address
- Medical information including allergies, medication, diagnoses, and individual healthcare plans
- Special Educational Needs and Disability (SEND) information and associated reports
- Attendance records, learning journals, and developmental assessments
- Free Nursery Entitlement claim data (shared with Bracknell Forest Council via secure electronic file transfer)
- Child Protection and safeguarding records (where applicable)
- Records of accidents, injuries, and incidents
- Information about involvement with Children's Social Care (CSC) or other external agencies

6.2 Parent and Carer Data

- Full names, home addresses, telephone numbers, and email addresses
- National Insurance numbers (for FNE claims)
- Emergency contact details
- Financial information relating to nursery fees and funding claims

6.3 Staff Data

- Full name, address, date of birth, and National Insurance number
- Bank details (for payroll purposes)
- Employment history, references, and right-to-work documentation
- Disclosure and Barring Service (DBS) check records — transmitted via secure file transfer to UKCRBs
- Training records, qualifications, and staff development reviews
- Disciplinary and grievance records (where applicable)

6.4 Visitor Data

- Full name, telephone number, address, and company name (where applicable)
- Date and time of visit

- Purpose of visit

This data is collected to fulfil our Health and Safety and Safeguarding obligations.

Lawful Bases for Processing — Summary

Data Category	Primary Lawful Basis	Notes
Children's records (general)	Legal obligation	EYFS Statutory Framework 2024, ss. 3.69–3.73
Children's health / SEND / CP records	Legal obligation + Vital interests (where applicable)	Article 9(2)(b) for special category data
Parent/carer contact and fee data	Contract	Registration agreement with the setting
Parent NI number (FNE claims)	Legal obligation	Free Nursery Entitlement regulatory requirements
Staff employment records	Contract + Legal obligation	Employment law, HMRC, DBS Code of Practice
Staff DBS data	Legal obligation	Childcare Act 2006 / EYFS suitability requirements
Visitor records	Legitimate interests	Health, Safety & Safeguarding obligations

Where special category data (Article 9) is processed, an additional condition under Schedule 1 of the Data Protection Act 2018 applies and is documented in the ROPA.

7. Sensitive (Special Category) Personal Data

The following categories of data are classified as special category data under Article 9 of the UK GDPR and require greater protection:

- Race and ethnicity
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical and mental health data
- Sexuality or sexual orientation
- Criminal offences and convictions

Special category data will only be processed where there is a clear and documented lawful basis, such as the explicit consent of the data subject, or where processing is necessary for the performance of obligations and the exercise of specific rights in the field of employment and social protection.

8. Rights of Individuals Under the UK GDPR

8.1 The Right to Be Informed

All parents, carers, staff, and visitors will be issued with a Privacy Notice at the point of data collection, explaining: what data we hold; why we hold it; how long we retain it; who we share it with; and how to exercise their rights.

8.2 The Right of Access — Subject Access Requests (SARs)

- Any individual may submit a Subject Access Request (SAR) to receive a copy of all personal data held about them.
- SARs must be submitted in writing to the DPO.
- The setting must respond within one calendar month of receipt.
- The response is free of charge unless the request is manifestly unfounded or excessive, in which case a reasonable fee or refusal may apply.
- Parents may submit SARs on behalf of their children. Where children are too young to consent, parents may submit on their behalf.
- Where we have a lawful obligation to retain data (e.g. from Ofsted under the EYFS), we must inform the individual of the reasons for any refusal to delete or provide.
- The individual has the right to complain to the ICO if they are not satisfied with the outcome.

8.3 The Right to Rectification

Individuals have the right to have inaccurate or incomplete personal data corrected. Requests must be made in writing to the DPO and actioned within one calendar month.

8.4 The Right to Erasure

Individuals may request deletion of their data where there is no compelling reason for its continued processing. However, Little Acorns Montessori Limited has legal duties to retain certain data for specified periods (see Section 10). Where erasure is refused on legal grounds, the individual will be informed in writing.

8.5 The Right to Restrict Processing

Parents, staff, and visitors may object to the processing of their data. Where processing is restricted, data may be stored but must not be used for any other purpose (e.g. reports, communications, or marketing) without consent.

8.6 The Right to Data Portability

Where data is transferred between IT systems — for example, from our Online Learning Journal to the Local Authority — data will be transmitted via secure file transfer. All recipient systems must have their own GDPR-compliant policies and procedures in place.

8.7 The Right to Object

Parents, staff, and visitors may object to their data being used for activities such as marketing, fundraising, or research. Such objections must be honoured promptly.

8.8 The Right Not to Be Subject to Automated Decision-Making

Little Acorns Montessori Limited does not use automated decision-making or profiling for any purpose.

9. Storage and Security of Personal Data

9.1 Paper Records

- All paper records relating to children and staff are stored in a locked office or locked filing cabinet at the relevant campus.
- Records must not be removed from the setting without written authorisation from the DPO.
- Files relating to individual children are confidential; information must not be left visible to other staff or parents.

9.2 Electronic Records

- All computers, laptops, tablets, and Online Learning Journals used by the setting are password protected.
- When a staff member leaves the setting, all associated passwords must be changed immediately, in line with this policy and the Safeguarding Policy.
- Any portable data storage devices (e.g. USB memory sticks) used to store personal data must be password protected and/or stored in a locked filing cabinet.
- Staff must not use personal devices to store, photograph, or transfer any setting-related personal data.

9.3 Data Shared with Third Parties

- Data shared with the Local Authority (e.g. Bracknell Forest Council), Ofsted, or schools is transmitted via a secure electronic file transfer system.
- Upon a child leaving the setting and transitioning to school, data may be shared with the receiving school via secure file transfer or at a School Transition Meeting.
- For children attending schools outside Bracknell Forest Council, the parent or carer will be given the data to deliver to the receiving school.
- All third-party recipients must operate their own GDPR-compliant data handling procedures.

9.4 Data Protection by Design and by Default

In accordance with Article 25 of the UK GDPR, Little Acorns Montessori Limited is committed to embedding data protection into all processes, systems, and projects from the outset — not as an afterthought.

In practice, this means:

- When selecting or implementing any new software, system, or process that involves personal data, the DPO must be consulted at the planning stage;
- Access to personal data will be limited by default to only those staff members who require it for their specific role (role-based access controls);

- New processing activities will be evaluated against the data minimisation principle before implementation;
- Where a new processing activity is likely to result in a high risk to individuals' rights and freedoms — particularly where special category data or children's data is involved — a Data Protection Impact Assessment (DPIA) must be completed before processing begins (see Section 9.5 below).

9.5 Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a structured process for identifying and minimising the data protection risks of a new or significantly changed processing activity. It is a legal requirement under Article 35 of the UK GDPR where processing is likely to result in a high risk to individuals.

Little Acorns Montessori Limited must carry out a DPIA before commencing any processing activity that:

- Involves large-scale processing of special category data (e.g. health, SEND, or safeguarding records);
- Introduces a new technology or software platform that processes children's or staff personal data;
- Involves systematic monitoring, profiling, or tracking of individuals;
- Represents a significant change to the way existing data is used or shared.

The DPO is responsible for:

- Screening all proposed new processing activities to determine whether a DPIA is required;
- Conducting or overseeing the DPIA process;
- Documenting the outcome and any mitigating actions taken;
- Retaining completed DPIAs as part of the setting's accountability records.

DPIAs are not a one-off exercise. The DPO will review existing DPIAs when circumstances change, new risks emerge, or new ICO guidance is published.

10. Data Retention Schedule

Personal data must not be retained for longer than is necessary for its purpose. The following retention periods apply. After the relevant retention period, all records must be securely shredded or permanently deleted.

Record Type	Retention Period	Authority / Notes
Standard children's records (registration, general correspondence, general developmental records)	Until age 21	Early Years Alliance / IRMS 2022
Accident / injury records (non-serious)	Until age 21 years and 3 months	Limitation Act 1980 / IRMS
Serious accident / hospitalisation records	Until age 21 years and 3 months	IRMS 2022
SEND records and healthcare plans	Until age 25	IRMS 2022 / SEND Code of Practice
Child Protection records (where CSC involvement, Section 47, Child in Need, or CP Plan)	Until age 25 (minimum)	IRMS 2022; DfE Data Protection Toolkit for Schools; Local Safeguarding Children Board requirements

Records relating to Looked After Children (LAC)	75 years	IICSA recommendation; IRMS 2022
Records relating to allegations or cases of child sexual abuse	75 years from date of allegation	Independent Inquiry into Child Sexual Abuse (IICSA)
Staff personnel files and training records	7 years after employment ceases	IRMS 2022
Staff DBS records	6 months after check is processed	DBS Code of Practice
Payroll records	7 years	HMRC requirements
Allegations against staff (investigated)	Until staff member reaches age 65, or 10 years — whichever is longer	IRMS 2022; even if allegations are unfounded
Visitor records / signing-in book	Up to 24 years (as part of safeguarding records)	Safeguarding obligation
Waiting list records (child did not attend)	Until confirmation child will not attend; then securely shredded	Data minimisation principle

IMPORTANT NOTE — Children Involved with Children's Social Care (CSC):

Where a child is the subject of a Child Protection Plan, a Child in Need Plan, a Section 47 enquiry, or any other formal CSC involvement, their records must be retained until the child reaches the age of 25 as a minimum. This retention period overrides the standard 'age 21' rule. Where a child has been Looked After (LAC), records must be retained for 75 years. The setting must keep these records in accordance with Bracknell Forest Local Safeguarding Children Partnership (LSCP) requirements.

11. Data Breach Reporting Procedure

A data breach is any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

11.1 Examples of Breaches

- Loss or theft of a device containing personal data
- Unauthorised access to records by a staff member or third party
- Sending personal data to the wrong recipient
- Personal data left accessible to visitors
- A cyberattack or ransomware incident affecting systems holding personal data

11.2 Immediate Response — All Staff

- Any suspected or actual data breach must be reported without delay to the DPO and Data Controller.
- Staff must not attempt to resolve a breach independently.
- The time and nature of the incident must be documented immediately.

11.3 DPO Action — Within 72 Hours

- The DPO must assess the risk to the rights and freedoms of individuals.
- If the breach is likely to result in a risk to individuals, it must be reported to the ICO within 72 hours of becoming aware of it, using the ICO online reporting tool at: https://ico.org.uk/
- If the breach is likely to result in a HIGH risk to individuals, affected individuals must also be notified directly and without undue delay.
- All breaches — including those not reported to the ICO — must be recorded in the Data Breach Register, regardless of severity.

11.4 Consequences of Breach

All breaches of information security policy will be investigated. Where investigations reveal misconduct, disciplinary action will follow in line with Little Acorns Montessori Limited's Disciplinary Procedures. Fines of up to £17.5 million or 4% of global annual turnover may be levied by the ICO under UK GDPR.

12. Privacy Notices

Little Acorns Montessori Limited must issue Privacy Notices to all data subjects at the point of data collection. Privacy Notices must explain:

- Who we are and how to contact us
- What personal data we collect and why
- Our lawful basis for processing
- How long we retain data
- Who we share data with
- The individual's rights under UK GDPR
- The right to lodge a complaint with the ICO

Separate Privacy Notices are issued for: children and parents/carers; staff and volunteers; visitors.

13. Photographs, Video, and Social Media

- Photographs and video recordings of children may only be taken on setting-owned devices.
- Personal mobile phones and devices must never be used to photograph or film children.
- Explicit written consent must be obtained from parents and carers before any images are used for any purpose, including the nursery website, newsletters, or social media.
- Consent can be withdrawn at any time; the setting must act promptly to remove images upon withdrawal.
- Images must be stored securely and must not be shared publicly without consent.

13.1 CCTV and Surveillance Systems

Where CCTV or other surveillance equipment is operated at any Little Acorns Montessori campus, the following requirements apply:

- A Data Protection Impact Assessment (DPIA) must be completed before any CCTV system is installed or materially changed (ICO Video Surveillance Guidance);
- Signage must be clearly displayed informing individuals that CCTV is in operation, the identity of the data controller, and the purpose of recording;
- CCTV footage must be stored securely, access restricted to authorised personnel only, and retained for no longer than 30 days unless required for an ongoing investigation or legal matter;

- CCTV footage must not be shared with third parties (including parents) without a lawful basis and authorisation from the DPO.

If Little Acorns Montessori Limited does not currently operate CCTV at any campus, this section will be reviewed and updated if surveillance equipment is introduced in future.

14. Staff Training and Awareness

- All new staff must complete data protection training as part of their induction, prior to accessing any personal data.
- All staff must complete refresher data protection training annually.
- The DPO must maintain a training log.
- Staff must be made aware of this policy and sign to confirm they have read and understood it.

15. Complaints and the ICO

Any individual who believes that Little Acorns Montessori Limited has failed to handle their personal data in accordance with UK GDPR has the right to raise a complaint with the DPO in the first instance.

If the matter is not resolved to their satisfaction, they have the right to lodge a complaint directly with the ICO:

- Website: https://ico.org.uk/
- Telephone: 0303 123 1113
- ICO Registration Reference for Little Acorns Montessori Limited: ZA161231

16. Legal and Statutory Framework

- UK General Data Protection Regulation (UK GDPR) — as amended by the Data (Use and Access) Act 2025 — https://ico.org.uk/ Data (Use and Access) Act 2025 (DUAA) — Royal Assent 19 June 2025 — https://www.legislation.gov.uk/ukpga/2025/16
- Data Protection Act 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Human Rights Act 1998
- The Children Act 1989 and 2004 (Every Child Matters)
- Childcare Act 2006
- Statutory Framework for the Early Years Foundation Stage (EYFS) 2024 — Sections 3.67–3.73
- Keeping Children Safe in Education (KCSIE) 2024
- Working Together to Safeguard Children 2023
- IRMS Records Retention Schedule for Education 2022
- Independent Inquiry into Child Sexual Abuse (IICSA) — Final Report 2022

17. Policy Review

This policy must be reviewed annually, or sooner in the event of:

- A change in relevant legislation or statutory guidance
- A significant data breach or ICO enforcement action

- A material change in the way personal data is collected or processed by the setting
- Ongoing changes to the UK data protection framework under the Data (Use and Access) Act 2025 (DUAA), including new ICO guidance, commencement regulations, or confirmed implementation dates for provisions not yet in force. The DPO is responsible for monitoring ICO DUAA updates and triggering an out-of-cycle policy review where a material change is identified.

18. Sign-Off

Role	Name	Date
Owner/Director	Jonathan Duffy	June 2026