35. Data Protection and Confidentiality Policy

Data protection, confidentiality, information sharing and individual rights

Mini Adventures | Updated September 2026 | Review September 2027

1. Purpose and scope

Mini Adventures holds personal information about children, parents/carers, staff, students, volunteers and other people connected with the setting. We will process personal information lawfully, fairly, securely and transparently and will only collect and use information that is necessary for identified purposes.

This policy should be read with the setting's Privacy Notice, records/retention schedule, safeguarding policy, staff confidentiality requirements and any relevant contracts or processor agreements.

2. Legal framework

UK GDPR and the Data Protection Act 2018.

Data (Use and Access) Act 2025 and associated changes to data protection law and ICO guidance.

EYFS statutory framework for group and school-based providers, including its requirements for secure records, confidentiality and parental access.

Relevant safeguarding legislation and Working Together to Safeguard Children 2026.

Other legislation requiring the setting to keep or share specific records.

The Freedom of Information Act 2000 does not generally apply to a private preschool as a public authority and has therefore been removed from this policy as a routine legal requirement.

3. Data protection principles

Lawfulness, fairness and transparency.

Purpose limitation – information is collected for specified, explicit and legitimate purposes.

Data minimisation – only information that is adequate, relevant and necessary is collected.

Accuracy – information is kept accurate and updated where necessary.

Storage limitation – information is not kept longer than necessary, subject to statutory, safeguarding, insurance and legal retention requirements.

Integrity and confidentiality – information is protected against unauthorised or unlawful processing, loss, destruction or damage.

Accountability – Mini Adventures must be able to demonstrate compliance.

4. Lawful processing

Mini Adventures will identify an appropriate lawful basis for each processing activity. Depending on the purpose, this may include contract, legal obligation, legitimate interests, vital interests or another lawful basis. Special category information, including health information and safeguarding information, also requires an applicable Article 9 condition. Consent will not be used as a blanket legal basis for all preschool processing.

Where consent is the appropriate basis – for example for certain optional photographs, publicity or other optional uses – consent will be specific, informed, freely given and capable of being withdrawn.

5. Information we may hold

Child name, date of birth, address, parent/carer and parental responsibility information and emergency contacts.

Attendance, collection arrangements, key-person information and relevant funding/administrative records.

Health, dietary, allergy, medication, first aid and other information necessary to keep children safe and well.

Learning and development information, SEND information and relevant professional reports.

Safeguarding and child protection records, which may need enhanced confidentiality and restricted access.

Photographs, videos and digital learning records where collected and used lawfully.

Staff and applicant information, including recruitment, DBS, qualification, reference, training and employment records.

6. Confidentiality and access

Paper records will be stored securely, including in locked storage where appropriate.

Electronic systems will be protected by appropriate passwords, access controls and security measures.

Staff, students and volunteers will receive confidentiality and data protection guidance as part of induction.

Information will only be shared internally with people who need it for their role.

Information will not be discussed in public places or with friends/family.

Safeguarding information will be shared promptly where necessary to protect a child; confidentiality does not override safeguarding duties.

Staff must report suspected data loss, unauthorised access or accidental disclosure immediately to management.

7. Parents' and children's rights

Parents/carers will normally be able to access records held about their child, subject to the Data Protection Act 2018 and other lawful exemptions. The right belongs to the child; whether a parent can exercise the right on the child's behalf depends on the child's age, maturity, competence and best interests.

Right to be informed through the setting's Privacy Notice.

Right of access to personal data (subject to exemptions).

Rights to rectification and, where applicable, restriction or objection.

Right to erasure in circumstances where the legal requirements are met; this is not an absolute right and does not override legal or safeguarding retention duties.

Other rights that may apply depending on the processing activity and lawful basis.

A subject access request can be made verbally or in writing. The setting will respond without undue delay and normally within one month. In complex or numerous requests, the response period may be extended by up to a further two months where permitted, with the requester informed within the original one-month period.

8. Safeguarding and information sharing

Where there is a safeguarding concern, information may be shared with children's social care, police, health professionals, safeguarding partners or other relevant agencies where there is a lawful basis. The setting will share information that is necessary, proportionate and relevant. Staff should seek DSL advice where practicable, but must not delay an urgent safeguarding referral.

Records relating to safeguarding may be retained for longer than ordinary administrative records where necessary for safeguarding, legal, regulatory, insurance or accountability purposes. The setting's retention schedule will specify retention periods.

9. Photographs, video and digital learning

Only authorised devices and approved systems may be used to photograph or record children.

Personal staff devices must not be used for storing or sharing children's images.

Images will be used only for purposes communicated to parents/carers and on an appropriate lawful basis.

Images uploaded to approved learning platforms such as Tapestry will be subject to account security and access controls.

Images will be deleted or retained in accordance with the relevant retention schedule and the purpose for which they were collected.

10. Data sharing with third parties

Where Mini Adventures uses external providers such as digital learning platforms, payroll providers, accountants, IT providers, funding systems or other processors, the setting will take reasonable steps to ensure appropriate contractual and security arrangements are in place and that personal data is processed only for authorised purposes.

International transfers will be managed in accordance with UK data protection law, including use of an appropriate transfer mechanism where required.

11. Data breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Staff must report suspected breaches immediately to management.

Management will contain and assess the incident promptly.

The setting will document the breach and the response.

Where required by law, the Information Commissioner's Office (ICO) will be notified without undue delay and, where feasible, within 72 hours of becoming aware of a notifiable breach.

Affected individuals will be informed where required by law because the breach presents a high risk to their rights and freedoms.

Lessons learned and preventative actions will be recorded.

12. Security

Paper records will be kept in secure storage and not left unattended where unauthorised people could access them.

Computers and accounts will use strong passwords and appropriate access controls.

Access rights will be limited to staff who need them and removed/changed when roles end or change.

Devices and systems will be kept appropriately updated and protected against malware where applicable.

Data will not be transferred using personal email accounts or unapproved messaging services unless an authorised secure method is being used.

Portable devices containing personal data will be protected against loss or unauthorised access.

13. Retention and disposal

Mini Adventures will maintain a separate records retention schedule identifying how long different categories of information are retained. Retention periods will take account of EYFS requirements, safeguarding, tax/funding, employment, insurance and other legal obligations.

Records will be securely destroyed or deleted when the retention period expires, unless there is a lawful reason to retain them longer.

Safeguarding records will be retained separately where appropriate and only for as long as justified by the safeguarding/legal purpose.

Backups and cloud systems will be managed so that deletion and retention arrangements are understood and proportionate.

14. Staff, students and volunteers

Confidentiality and data protection form part of induction.

Staff must not discuss personal information outside the setting or with people who do not need to know.

Employment and recruitment records are confidential and access is restricted.

Staff may request access to their own personal information in accordance with data protection law.

Serious breaches of confidentiality may result in disciplinary action.

15. Privacy notice and transparency

The setting will maintain a clear Privacy Notice explaining what information is collected, why it is used, lawful bases, who it is shared with, retention, individual rights and how to contact the setting about data protection. The Privacy Notice will be made readily available to parents, carers and staff and kept under review.

16. ICO and complaints

Mini Adventures will maintain any ICO registration/fee obligations that apply to its processing activities. Individuals may raise data protection concerns with the setting first and may complain to the Information Commissioner's Office where appropriate.

Information Commissioner's Office: ico.org.uk

17. Review

This policy will be reviewed annually and sooner if data protection law, ICO guidance, EYFS requirements or the setting's systems change.

Policy adopted: 28/01/2026 (original policy record). Updated: September 2026. Next review: September 2027.