

Data Protection and Confidentiality

Little Lanes Out of School Club | October 2026

Purpose and responsibilities

Little Lanes respects the privacy of children, families, staff and volunteers. We collect and use personal information fairly, keep it secure and share it only for a lawful purpose. This policy covers paper records, iPAL, email, photographs and information held on computers or authorised phones. It follows the UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, and applicable EYFS requirements.

Clare Greenham, Megan Garratt and Cheri Garratt oversee data protection. Megan is the first contact for requests and complaints; Clare or Cheri provides cover or handles concerns involving Megan. These are operational lead responsibilities, not an assertion that a statutory Data Protection Officer has been appointed. All staff, students and volunteers must follow this policy, including after leaving the Club.

Contact Megan: littlelanesoosc@hotmail.com. Alternatively, call Cheri on 07950 875097 or speak privately to a manager. Where a concern involves someone with access to the email account, request a confidential alternative from another lead.

Information we hold and why

- Children and families: registration and contact details, bookings, attendance, authorised collectors, relevant medical and allergy information, support plans, permissions and accident, incident or safeguarding records.
- Staff, applicants and volunteers: recruitment and suitability checks, employment, payroll, training, emergency contacts and relevant health or adjustment information.
- Administration: payment records, complaints, visitor records and necessary correspondence. Collect only what is needed and keep factual records accurate and up to date.

Management maintains a record of the information held, its purpose, lawful basis, access, recipients and retention period. An iPAL booking record alone is not a complete record of all the Club's data processing. Families and staff receive accessible privacy information explaining how their information is used and how to exercise their rights.

Lawful use of information

Identify and record an appropriate lawful basis for each purpose before processing. This may include contract for a parent's booking, legal obligation for required records, or legitimate interests where justified and balanced against the individual's rights. A parent's contract does not automatically provide the basis for every use of a child's information. Use consent only where it is appropriate and can be freely given and withdrawn.

Health, disability and other special category information also require a specific Article 9 condition and any applicable Data Protection Act Schedule 1 condition. Management must record the condition and maintain an appropriate policy document where required. "Providing care" alone is not a complete legal condition. Criminal record information also requires the relevant legal authority and safeguards.

Optional photograph permissions must be specific. Refusing optional photographs does not affect a child's place. Follow the Mobile Phones, Online Safety and Photographs Policy; do not introduce public website or social-media use without a separate review and appropriate permissions.

Keeping and sharing information safely

Confidentiality in daily practice

- Discuss children only where necessary to care for or protect them, and where conversations cannot be overheard by other families. Do not disclose another child's or family's private information when discussing an incident.
- Give staff the information they need for their duties. Safeguarding records have restricted access, but essential protective instructions must reach the staff who need them; confidentiality must not prevent safe care.
- Keep employment matters private and limit access to authorised staff. Do not use personal information for curiosity, gossip or an unrelated purpose.
- Keep the live register readily available to staff for supervision and evacuation, while shielding it from casual viewing. Keep medical lists inside the cupboard and accessible only to those who need them.

Paper records and electronic security

- Store confidential files in locked storage when not in use. Return records promptly, control keys and avoid leaving folders, medication records or printed lists unattended or visible to visitors.
- Use individual accounts where available, strong unique passwords, multi-factor authentication where supported, screen locks, current security updates and device encryption. Lock the laptop whenever unattended and keep screens away from public view.
- Restrict iPAL and other systems to authorised users, review access when roles change and remove it promptly when staff leave. Maintain appropriate backups and check that essential records can be recovered.
- Megan Garratt is authorised to access iPAL and carry out Club administration from home using her secured laptop, and to use her authorised phone for work purposes in accordance with the Mobile Phones Policy. Devices must be password protected, kept updated and locked when unattended. Club information must be protected from access by family members or other unauthorised people. Any necessary downloads or copies must be stored securely, must not be saved to unapproved personal cloud accounts and must be deleted when no longer required under the Club's retention arrangements.
- Check recipients and attachments before sending. Use individual messages or BCC for group emails where addresses should remain private. Send sensitive records through an approved secure method; where encrypted attachments are used, share the password separately.
- Do not upload identifiable child, family or staff records to unapproved apps, AI tools, personal storage or messaging groups. Report lost devices, suspicious messages or accidental disclosures immediately.

Sharing with school and other organisations

Little Lanes and the school are separate organisations. Agree the purpose, relevant information, secure method and responsibilities for routine handover or support information. Explain routine sharing to families and obtain consent where that is the appropriate basis. Do not promise that every disclosure depends on parental permission.

Share necessary, relevant and proportionate information with safeguarding agencies or other authorised recipients when a lawful basis permits or requires it. Do not delay necessary safeguarding action while seeking consent. Record significant sharing decisions, reasons, recipients and what was shared. Check identity and authority before releasing information, including to someone claiming to represent an official body.

Before using a service provider such as a booking, email or payroll provider, management checks its security and data-protection arrangements. Put appropriate processor contracts in place where required, consider international transfers and assess higher-risk new processing before introducing it.

Retention rights and data incidents

Keeping records for the right length of time

Management maintains a retention schedule for each record type, reflecting statutory duties, safeguarding needs, relevant claims periods and insurer requirements. Do not keep everything indefinitely or apply one blanket period to every record. Review records regularly, including downloads, email attachments and paper copies.

Preserve information needed for an active safeguarding matter, complaint, investigation or legal claim. When retention ends, securely shred paper and securely delete electronic copies through the relevant system, including managed backup cycles. Do not place identifiable records in ordinary waste. Keep a record of significant disposal decisions.

Requests to see or change information

People may request access, correction, erasure, restriction, portability or object to processing where the relevant right applies. Requests can be verbal or written and do not need legal wording or a special form. Staff must record and forward them promptly to a data protection lead; do not wait until the end of the week.

For subject access, respond without undue delay and normally within one calendar month. Only request identity or authority evidence where needed and do so promptly. Where the law permits an extension for complexity or multiple requests, explain the reason within the original deadline; the extension may be up to two further months. Any permitted clarification pause must follow current ICO guidance and be recorded. Requests are normally free.

The right to a child's information belongs to the child. Before responding to a parent or representative, consider their authority, the child's understanding and wishes, the child's best interests and any relevant restrictions. Parental responsibility does not automatically mean unrestricted access to every record. Protect other people's information and apply exemptions only where justified, seeking advice where necessary.

Correct inaccurate information promptly. Where a historical record must remain, add an accurate correction or clarification. Erasure is not absolute: explain any lawful reason for keeping information and the right to complain. Assess requests individually rather than automatically threatening to end childcare or employment.

Loss disclosure or another personal data breach

A breach can include a lost register, an email sent to the wrong person, unauthorised access, loss of availability or accidental deletion. Staff must tell a lead immediately, preserve relevant evidence and follow instructions to contain the incident. Do not conceal it or try to resolve a serious incident alone.

- Management records what happened, when the Club became aware, affected information and individuals, likely harm, containment and corrective action. Record all breaches, including those not reported to the ICO.
- Notify the ICO without undue delay and within 72 hours of awareness where the breach is likely to pose a risk to people's rights and freedoms. Report available facts first if necessary and supply further details later; explain any delay.
- Where the breach is likely to create a high risk, inform affected people without undue delay unless a lawful exception applies. Explain clearly what happened, likely effects, protective steps and a contact point.
- Involve the DSL immediately where a child's safety could be affected. Review the cause and improve controls or training. Record reasons for reporting or not reporting.

Data protection complaints

How to raise a concern

Anyone can complain about how Little Lanes handles their personal information, including access requests, sharing, accuracy, retention, photographs or security. Contact Megan by email, call Cheri, speak to staff or write to the Club. We also accept an authorised representative's complaint and provide reasonable help to make a complaint. No special wording or form is required.

Receipt and acknowledgement

Staff record the date received and forward the complaint to a data protection lead within one working day, or immediately if there is a security or safeguarding risk. Allocate a reference, preserve relevant records and check identity or representative authority only where necessary.

We aim to acknowledge promptly and must do so within 30 calendar days of receipt. The count begins the day after receipt; if the deadline falls on a weekend or public holiday, the next working day applies. The acknowledgement confirms the concern, reference, lead contact and investigation process. Investigation starts on receipt, not after the acknowledgement deadline.

Investigation and updates

The lead investigates without undue delay, proportionately to the nature and potential impact of the concern. This may include checking records and systems, speaking to staff, consulting service providers and reviewing relevant procedures. Ask for clarification where needed without making assumptions or requesting unnecessary personal information.

Keep the complainant informed without undue delay. Where the matter remains open, the Club will provide an update at least every 30 days, even if there is little progress. This is our update standard, not an extension of any separate legal deadline. A subject access request, reportable breach or EYFS complaint must still meet its own applicable timescale.

Outcome and escalation

Provide a written outcome without undue delay, explaining the concern considered, findings, reasons and any corrective action. If the complaint is not upheld, explain why. The 30-day acknowledgement rule is not a fixed deadline for the final outcome; do not allow an investigation to drift unnecessarily.

Explain that the person can complain to the Information Commissioner's Office if dissatisfied: ico.org.uk/make-a-complaint or telephone 0303 123 1113. Provide these details in the final response. Where a complaint concerns a lead, another lead should handle it; seek independent advice where necessary.

Records training and review

Keep a restricted complaints register showing the reference, dates received and acknowledged, concern, investigation, updates, outcome, closure and lessons or actions. Retain it under the documented retention schedule; six years is not a universal data-protection requirement. Brief staff at induction and when procedures change. Management reviews compliance, privacy notices, access controls and retention arrangements regularly and checks whether an ICO data protection fee is payable.

Approval

Adopted by: Little Lanes Out of School Club

Date approved: October 2026 Review date: October 2027

Signed:MG Name and role: Megan Garratt - Manager

Review annually and sooner following changes in law, systems or Club practice. Read alongside Safeguarding; Complaints; Staff Code of Conduct; Mobile Phones, Online Safety and Photographs; Whistleblowing and Safer Recruitment.

Sources: UK GDPR and Data Protection Act 2018 as amended; ICO guidance on complaints, subject access, special category data and personal data breaches (ico.org.uk); current EYFS framework.