



Information Sharing, Confidentiality and Data Protection Policy

1. Purpose

The Life Nursery is committed to protecting the privacy, confidentiality and personal information of children, parents/carers, staff, students, volunteers and other individuals connected with the setting.

The purpose of this policy is to ensure that information is:

- collected, stored and used lawfully, fairly and transparently;
- kept confidential and secure;
- only shared when there is a legitimate and appropriate reason to do so;
- shared in a timely manner where necessary to protect a child or another person from harm;
- shared on a need-to-know basis;
- accurate, relevant and up to date;
- retained only for as long as necessary; and
- handled in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant legislation and guidance.

The nursery recognises that protecting children's personal information is particularly important because children may be less aware of the risks associated with their personal information.

2. Scope

This policy applies to everyone working at or for the nursery, including:

- permanent and temporary employees;
- managers and directors
- agency workers;
- students and apprentices;
- volunteers;
- contractors and visitors where appropriate.

It applies to information held in:

- paper records;
- electronic systems;
- emails and messaging systems;
- photographs and videos;
- mobile phones and tablets;
- safeguarding records;
- attendance and registration systems; and
- any other format containing personal information.

3. What is confidential information?

Confidential information includes any information about a child, family, staff member or other individual that is not intended for general access.

Examples include:

- children's names, addresses and contact details;
- dates of birth;
- medical and allergy information;
- medication records;
- developmental information;
- observations and assessments;
- Special Educational Needs and Disabilities (SEND) information;
- safeguarding concerns and records;
- information about family circumstances;
- social care involvement;
- information relating to domestic abuse or other risks;
- court orders and information about parental responsibility;
- photographs and videos;
- staff personal information;
- complaints and disciplinary information; and
- any information that could identify an individual.

Staff must treat confidential information with respect and must not discuss information about children or families inappropriately.

4. Confidentiality

All staff have a professional responsibility to maintain confidentiality.

Information about children and families must only be discussed with colleagues who need the information to carry out their role safely and effectively.

Staff must not:

- discuss children or families in public areas;
- discuss confidential matters with friends or family members;
- discuss one child's circumstances with another child's parent/carer;
- share information on social media;
- take confidential documents away from the nursery without authorisation;
- leave confidential information unattended;
- disclose passwords or login details; or
- access records that they do not need for their role.

Confidential information must not be discussed with parents/carers about other children or families.

For example, if a parent asks why another child has additional support or why a particular incident occurred, staff must explain that information about other children is confidential and cannot be disclosed.

5. Information sharing within the nursery

Information should be shared internally where it is necessary for the effective care, education, health, development or safeguarding of a child.

Staff should share information on a **need-to-know basis** rather than routinely sharing all information.

For example, relevant information may need to be shared with:

- the child's key person;
- the Designated Safeguarding Lead (DSL);
- the nursery manager;

- a SENCO;
- another member of staff responsible for the child's care;
- another appropriate professional.

Staff should not assume that confidentiality means information can never be shared.

Where there is a safeguarding concern, information must be passed promptly to the DSL or, where appropriate, directly to the relevant safeguarding agency.

6. Information sharing for safeguarding

The nursery recognises that effective information sharing is an essential part of safeguarding children.

Data protection law does **not** prevent appropriate information sharing when it is necessary to protect a child from harm. The ICO specifically recognises safeguarding as a compelling reason for sharing children's personal information.

Where there is a concern that a child may be suffering, or may be at risk of suffering, significant harm, staff must follow the nursery's Safeguarding and Child Protection Policy.

Information may need to be shared with relevant agencies, including:

- Children's Social Care;
- the Local Authority Designated Officer (LADO), where appropriate;
- the police;
- health professionals;
- the child's school or other educational setting;
- the local safeguarding partnership;
- Ofsted or another regulatory body where required; or
- another appropriate agency.

Staff should not delay sharing information because they are unsure whether consent has been obtained where doing so could place a child at further risk.

Where appropriate, the DSL/manager will make decisions about information sharing. However, staff must immediately report safeguarding concerns and must not wait for permission from a manager if doing so would place a child at risk.

7. Consent and information sharing

Consent will be obtained where consent is the appropriate lawful basis for processing or sharing information.

However, staff must understand that **consent is not required for every type of information sharing**.

There may be circumstances where information can or must be shared because of:

- a legal obligation;
- safeguarding responsibilities;
- the vital interests of a child or an individual;
- another lawful basis under data protection legislation; or
- another legal requirement or power to disclose information.

The nursery will not rely on consent where another lawful basis is more appropriate.

Where information is shared for safeguarding purposes, the child's best interests will be a primary consideration.

8. Sharing information with parents and carers

Parents/carers will normally be provided with appropriate information about their child's care, development, learning, health and wellbeing.

However, parental responsibility does not automatically mean that a parent/carer is entitled to receive all information held by the nursery.

Before disclosing information, the nursery will consider:

- whether the person has parental responsibility;
- whether the request concerns information about their own child;
- whether another person's information is contained within the records;
- whether there are safeguarding concerns;
- whether disclosure would be in the child's best interests;
- whether there are court orders or other legal restrictions; and
- whether there is another lawful reason preventing disclosure.

Where there are safeguarding concerns, the nursery may withhold information or seek advice from the relevant safeguarding authority before disclosure.

The ICO advises that requests for children's information made by parents or representatives should be considered carefully, including whether disclosure is appropriate and in the child's best interests.

9. Data protection principles

The nursery will follow the data protection principles when handling personal information.

Personal information will be:

1. **Processed lawfully, fairly and transparently.**
2. **Collected for specified, explicit and legitimate purposes.**
3. **Adequate, relevant and limited to what is necessary.**
4. **Accurate and kept up to date where necessary.**
5. **Kept only for as long as necessary.**
6. **Kept secure and protected against unauthorised or unlawful processing, loss, destruction or damage.**

The nursery will also maintain appropriate records and procedures to demonstrate compliance with data protection requirements.

10. Special category information

The nursery may process information that requires additional protection, including:

- health information;
- medical conditions;
- allergies;
- disability/SEND information;
- safeguarding information; and
- other special category information where applicable.

Access to this information will be restricted to staff who need it to perform their duties.

Additional safeguards will be used where appropriate.

11. Keeping information secure

The nursery will take appropriate organisational measures to protect personal information.

This includes:

- locking paper records away;
- using secure passwords;
- restricting access to electronic systems;
- not sharing passwords;
- locking computers when unattended;
- keeping mobile devices secure;
- using secure methods to transfer sensitive information eg galaxkey
- checking email addresses carefully before sending information;
- using encryption or other appropriate security measures for sensitive electronic information;
- securely disposing of confidential documents; and
- regularly reviewing staff access to information.

The ICO specifically recommends appropriate physical and electronic security measures for early years settings, including locked filing cabinets, password-protected computers and additional safeguards when sending sensitive information.

12. Emails and electronic communication

Staff must take particular care when sending personal or confidential information by email.

Before sending an email containing personal information, staff should:

- check the recipient's email address carefully;
- ensure that only necessary information is included;
- avoid including unnecessary sensitive information;
- use secure/encrypted methods where appropriate;
- consider whether an attachment is necessary; and
- check that information is being sent to the correct person.

Confidential information must not be sent to personal email accounts unless specifically authorised and appropriate safeguards are in place.

13. Mobile phones, photographs and videos

Photographs and videos of children are personal information and must be handled appropriately.

The nursery will ensure that:

- photographs are taken only for legitimate nursery purposes;
- staff use nursery-approved devices wherever possible;
- personal mobile phones are not used to photograph children
- photographs are stored securely;
- photographs are not shared through personal social media accounts;
- images are not shared with other parents
- photographs are deleted or securely disposed of when no longer required; and
- parental permissions and the nursery's privacy information are kept up to date.

14. Social media

Staff must never share confidential information about children, families or colleagues on social media.

Staff must not:

- post photographs of children from the nursery on personal accounts;
- identify children or families in posts;
- discuss safeguarding concerns;
- discuss confidential incidents;
- post screenshots of nursery records or messages; or
- make comments that could identify a child or family.

Staff should also be mindful that information shared outside work can affect professional confidentiality and the reputation of the nursery.

15. Data breaches

A personal data breach may include:

- sending information to the wrong person;
- losing a laptop, tablet or phone containing personal information;
- losing paper records;
- unauthorised access to records;
- accidental disclosure of confidential information;
- hacking or cyberattack;
- theft; or
- accidentally deleting or altering personal information.

All suspected or actual data breaches must be reported to the nursery Manager immediately.

Staff must not attempt to conceal a data breach.

The nursery will assess the breach and take appropriate action, including determining whether it needs to be reported to the Information Commissioner's Office (ICO) and/or affected individuals.

16. Subject access requests and individual rights

Individuals have rights regarding their personal information under data protection legislation.

These may include rights relating to:

- access to personal information;
- correction of inaccurate information;
- restriction of processing;
- objection to processing;
- erasure in certain circumstances; and
- data portability where applicable.

Children have data protection rights too, although how these rights are exercised can depend on the child's age, maturity and understanding.

Any request for access to personal information should be passed to the nursery Manager without delay.

Staff must not provide records directly unless authorised to do so by the Manager.

17. Data retention

The nursery will not keep personal information indefinitely.

Information will be retained only for as long as necessary for:

- the purpose for which it was collected;
- legal or regulatory requirements;
- safeguarding requirements;
- accounting or employment requirements; or
- another legitimate purpose.

The nursery will maintain an appropriate retention schedule identifying how long different categories of information should be retained.

At the end of the retention period, information will be securely destroyed or deleted.

18. Sharing information with external organisations

Before sharing information with another organisation, the nursery will consider:

1. What information needs to be shared?
2. Why does it need to be shared?
3. Is there a lawful basis for sharing?
4. Is the information necessary and proportionate?
5. Is sharing in the child's best interests?
6. Who needs to receive the information?
7. How will the information be transferred securely?
8. Is there a legal or safeguarding requirement to share?
9. What records need to be made of the decision?

The nursery will carry out appropriate checks and due diligence when sharing information with third-party organisations. The ICO recommends particular care when children's data is shared with third parties and advises that risks to children's rights and freedoms should be considered.

19. Staff training

All staff will receive appropriate induction training and guidance on:

- confidentiality;
- data protection;
- information sharing;
- safeguarding;
- handling personal information;
- secure use of electronic systems;
- social media;
- photographs and videos; and
- reporting data breaches.

Staff are expected to understand their individual responsibilities and to seek advice from the manager/DSL if they are unsure whether information can or should be shared.

20. Record keeping

Where a significant decision to share or withhold information is made, an appropriate record should be kept.

The record should include, where appropriate:

- what information was shared or withheld;
- why it was shared or withheld;
- who it was shared with;
- the lawful basis or other justification;
- whether consent was sought;
- whether consent was refused or could not reasonably be obtained;
- any safeguarding considerations; and
- the date and person making the decision.

Records should be factual, accurate and professional.

21. Responsibilities

Nursery Manager/Directors

The Manager/Directors are responsible for ensuring that:

- appropriate data protection procedures are in place;
- staff receive suitable training;
- personal information is kept secure;
- data breaches are dealt with appropriately;
- data protection policies are reviewed;
- appropriate records are maintained; and
- external advice is obtained where necessary.

Designated Safeguarding Lead

The DSL is responsible for ensuring that information relating to safeguarding concerns is shared appropriately and promptly in accordance with safeguarding procedures.

The DSL will ensure that staff understand that confidentiality must never prevent necessary safeguarding action.

All staff

All staff are responsible for:

- maintaining confidentiality;
- following this policy;
- only accessing information they need;
- keeping information secure;
- reporting concerns promptly;
- reporting data breaches immediately; and
- seeking advice if they are unsure about sharing information.

22. Information sharing decision-making procedure

When deciding whether to share information, staff should consider:

1. Is there a safeguarding concern?

If yes, follow the nursery safeguarding procedure and speak to the DSL immediately.

2. Is there a legitimate reason to share the information?

Identify the purpose and appropriate lawful basis.

3. Is the information necessary?

Only share information that is relevant and proportionate.

4. Who needs the information?

Share only with appropriate individuals or organisations.

5. Would delaying the sharing of information put a child or another person at risk?

If yes, information should be shared promptly with the appropriate person/agency.

6. How can the information be shared securely?

Use an appropriate secure method.

7. Has the decision been recorded where necessary?

Make a clear, factual record of significant information-sharing decisions.

23. Confidentiality and safeguarding

The nursery recognises that confidentiality is important but is **not absolute**.

Information may need to be shared without the consent of a parent/carer where this is necessary to protect a child or another person from harm, or where there is another lawful basis or legal requirement to share.

Staff must never promise a child, parent or colleague that information will be kept completely secret if there is a possibility that it may need to be shared to protect someone from harm.

Where a child discloses information indicating a safeguarding concern, staff must follow the nursery's Safeguarding and Child Protection Policy and report the concern to the DSL without delay.

24. Compliance and review

This policy will be reviewed at least annually or sooner where there are:

- changes to legislation;
- changes to government or ICO guidance;
- significant changes to nursery procedures;
- a data breach or incident indicating that changes are required; or
- changes to the systems used to store or share information.

Policy reviewed by Louise Gray, Nursery Manager– October 2026

Policy read and agreed by: