Confidentiality and Data Protection Policy

1. Purpose and scope

This policy sets out how we collect, store, use, share and protect personal information relating to children, families, staff and visitors. It ensures confidentiality, safeguards children's welfare and complies with data protection legislation.

This policy applies to:

- All staff, students, volunteers, agency staff and visitors
- All children and families using the setting
- All paper and electronic records, images, devices and online systems

2. Legal framework

This policy is informed by and complies with:

- The Early Years Foundation Stage (EYFS) statutory framework
- The Education Inspection Framework (EIF)
- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000

Safeguarding and child protection requirements override confidentiality where a child may be at risk of harm.

3. Data protection principles

All personal data is processed in accordance with UK GDPR principles. We ensure that data is:

- Processed lawfully, fairly and transparently
- Collected for specific, legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Retained only as long as required

- Kept secure against unauthorised access, loss or misuse

---

4. Types of data we hold

We may hold personal data including:

- Names, addresses and contact details
- Emergency contacts
- Medical, health, disability, allergy and dietary information
- Cultural or religious requirements
- Accident, incident and safeguarding records
- Developmental observations and learning records
- Photographs and videos
- Funding and eligibility information
- Staff employment and suitability records

Special category data (e.g. health or safeguarding information) is processed only where legally permitted.

---

5. Lawful basis for processing

We process personal data under one or more of the following lawful bases:

- Legal obligation (EYFS, safeguarding, funding)
- Contract (delivery of early years provision)
- Legitimate interests (safe and effective operation of the setting)
- Consent (e.g. photographs, marketing). Consent may be withdrawn at any time.

---

6. Confidentiality and staff conduct

- Information is shared strictly on a need-to-know basis
- Staff must not discuss confidential information outside the setting or in public places
- Information accessed through a staff role must only be used for professional purposes
- Breaches of confidentiality may result in disciplinary action
- Employment matters remain confidential to those involved in decision-making

---

7. Access to records

- Parents/carers may access records relating to their own child, unless doing so would place the child at risk or is restricted by external agencies
- Records relating to other children or third parties will not be shared
- Fulfilling requests from other professionals require parental consent unless safeguarding legislation applies

---

8. Information storage and security

- Paper records are stored in locked cabinets.
- Electronic records are stored on secure, password-protected systems.
- Devices are locked when unattended and access is restricted.
- Children's records are not removed from the premises without authorisation.
- Cyber security risks are assessed and managed appropriately.

---

9. Photography, images and digital media

- Written parental consent is obtained for the use of images
- Only setting-owned devices are used to take photographs or videos
- Images are stored securely and shared only via approved systems ie Ovivio
- Staff must not store or share images on personal devices or accounts
- Parents may be allowed to photograph other children at events but any photographs featuring other children must not be shared in any form including social media
- Livestreaming is not permitted
- Approved digital systems are subject to data processing agreements and Snug Nursery Schools due diligence

---

10. Use of technology and online systems

- Technology is used appropriately to support children's learning and development
- Children are supervised at all times when using digital devices
- Online content is age-appropriate and pre-checked
- Open internet access is not provided to children and Wi-Fi restrictions are in place to prevent the use of inappropriate websites
- Professional boundaries must be maintained online; staff must not connect with families via personal social media

- Devices must remain on nursery premises unless taken on an outing where they should be assigned to a member of staff who must take responsibility for that device whilst away from the nursery
- Any missing devices must be remotely wiped immediately upon reporting
- All devices should be protected with a password
- CCTV is not used either inside or outside of our nurseries

---

11. Data sharing and safeguarding

Information may be shared with:

- Local authority services
- Safeguarding partners
- Health or education professionals

This is done lawfully, proportionately and in the child's best interests. Where a child may be at risk, safeguarding procedures take precedence over confidentiality.

Parents receive the privacy notice when they register at the nursery. It is also available to them on Ovivio and on the nursery website.

---

12. Data retention

We retain data only as long as required by law or guidance, including:

- Children's records: until the child reaches 21 years
- Safeguarding records: 24 years
- Photographs: retained only in learning records on Ovivio or for a limited period where not required

Records are disposed of securely.

---

13. Data subject rights

Parents/carers and staff have the right to:

- Be informed about how data is used
- Access their personal data
- Request correction or erasure (where applicable)
- Restrict or object to processing
- Data portability
- Complain to the Information Commissioner's Office (ICO)

- Any Subject Access Requests responded to within one calendar month, subject to safeguarding exemptions where applicable

---

14. Training and awareness

- All staff receive data protection and confidentiality training as part of their induction
- Training is refreshed regularly through supervision and professional development
- Staff understand reporting procedures for breaches or concerns

---

15. Breaches and incidents

Any data breach or concern involving:

- Loss or unauthorised access to data
- Misuse of images or devices
- Online safety concerns

must be reported immediately to the manager/DSL and responded to in line with safeguarding and data protection procedures.

The nursery manager will decide whether the data breach meets the threshold for reporting to the ICO and will act accordingly within 72 hours.

Policy date: March 2026
Next review: March 2027

Appendix 1

Education Inspection Framework (EIF)

Intent – Implementation – Impact Summary

Intent *(Why)*

To ensure all personal information is handled lawfully, securely and respectfully, supporting children's safety, wellbeing and rights while maintaining trust with families and staff.

Implementation *(How)*

- Clear policies and procedures understood by all staff
- Secure systems and controlled access to information
- Regular training, supervision and oversight
- Strong safeguarding leadership and reporting culture

Impact *(What difference it makes)*

- Children's information is protected and used appropriately
- Families have confidence in how information is managed
- Staff demonstrate secure, professional practice
- The setting meets EYFS and GDPR requirements and demonstrates exemplary safeguarding practice under the EIF