Confidentiality Policy

1. Policy Statement

Stowey Bears Preschool is committed to maintaining the **highest standards of confidentiality** in order to protect children, families, and staff. We recognise that trust is central to effective relationships and that sensitive information must be handled lawfully, securely, and with professional integrity. Confidentiality is a core safeguarding expectation and forms part of our duty under the **EYFS 2024**, **Data Protection Act 2018**, **UK GDPR**, and **KCSIE 2024**.

2. Aims

- To ensure all personal information is handled securely, lawfully, and transparently.
- To protect children and families from harm, stigma, or inappropriate disclosure.
- To ensure staff understand their responsibilities regarding confidentiality and information sharing.
- To ensure information is shared appropriately when it is necessary to safeguard a child.

3. Legal and Statutory Framework

This policy is informed by:

- **Early Years Foundation Stage (EYFS) 2024**
- **Data Protection Act 2018 & UK GDPR**
- **Working Together to Safeguard Children 2023**
- **Keeping Children Safe in Education (KCSIE) 2024**
- **Information Sharing Advice for Practitioners (DfE)**
- **Local Authority Designated Officer (LADO) procedures**

4. What We Class as Confidential Information

Confidential information includes, but is not limited to:

- Child records, learning journals, assessments, SEND information
- Safeguarding concerns, disclosures, referrals, and multi-agency documents
- Family circumstances, health information, court orders
- Staff records, supervision notes, and HR information
- Contact details and personal identifiers
- Photographs, videos, and digital data

5. How We Store and Protect Information

- All paper records are stored in **locked cabinets** accessible only to authorised staff.
- Digital records are stored on **secure, password-protected systems** (e.g., Tapestry, secure drives).
- Only staff with a legitimate professional need can access information.
- Personal data is retained and disposed of in line with our **Data Retention Schedule** and **Somerset Council guidance**.
- Staff must never store confidential information on personal devices.

6. Staff Responsibilities

All staff must:

- Maintain confidentiality at all times, including outside working hours.
- Never discuss children or families outside the professional context.
- Never share information with other parents, visitors, or unauthorised individuals.
- Follow the setting's safeguarding procedures when information indicates a child may be at risk.
- Report any data breach immediately to the Manager/DSL.

Staff sign a **Confidentiality Agreement** as part of induction and annually thereafter.

7. Information Sharing

We share information only when:

- It is necessary to **safeguard a child**.
- It is required by law (e.g., court order, police request).
- It supports a child's learning, development, or wellbeing.
- Parents/carers have given **informed consent**, unless doing so would place a child at risk.

When sharing information, we follow the **7 Golden Rules of Information Sharing (DfE)**.

8. Safeguarding Exception

Confidentiality **must never** prevent staff from taking action to safeguard a child. Information will be shared with:

- **Children's Social Care**
- **Police**
- **Health professionals**
- **LADO** (for allegations against staff)
- Other relevant agencies

Parents may not be informed if doing so could increase risk to the child.

9. Working with External Agencies

When working with health visitors, SENCOs, social workers, or other professionals:

- Only relevant information is shared.
- Information is transferred securely.
- Records of what was shared, with whom, and why are kept.

10. Breaches of Confidentiality

A breach includes:

- Sharing information inappropriately
- Leaving documents unsecured
- Discussing children in public areas
- Using personal devices to store or share information

Breaches will be investigated and may result in:

- Additional training
- Formal disciplinary action
- Referral to LADO (if safeguarding related)

11. Confidentiality and Parents/Carers

Parents/carers:

- Have the right to access their child's records (subject to safeguarding restrictions).
- Will not have access to information about other children or families.
- Will be informed about how their data is stored and used.

12. Confidentiality and Students/Volunteers

Students and volunteers:

- Are given only the information necessary for their role.
- Must never remove or copy records.
- Must follow this policy and sign a confidentiality agreement.

13. Photography, Video and Digital Media

- Images are only taken on **setting-owned devices**.
- Images are stored securely and deleted in line with retention procedures.
- Parental consent is required for any use beyond internal documentation.

(Links with: Mobile Phones, Cameras and Smart Watches Policy)

14. Record Keeping and Retention

We follow Somerset Council and statutory retention schedules, including:

- Safeguarding records: **until the child is 25**
- Accident/incident forms: **21 years + 3 months**
- General child records: **reasonable period as per EYFS and LA guidance**

15. Monitoring and Review

This policy is reviewed **annually** or sooner if:

- Legislation changes
- There is a data breach
- Ofsted or LA guidance changes
- A safeguarding review identifies improvements

Reviewed by: Rachel Penny (Manager/DSL) **Approved by:** Julia Jameson (Chairperson) **Next Review Due:** September 2027