OPERATIONAL PLAN STANDARD 4 - CONFIDENTIALITY AND RECORD-KEEPING
Supporting Documentation S4.2 GDPR and Record Keeping Policy and Procedure

Policy Statement:
At Kaleidoscope nursery, we are committed to ensuring that all personal data, information sharing, and record-keeping practices are carried out in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. We recognise that maintaining the confidentiality, integrity, and security of personal data is essential to building trust with children, families, and staff. This policy also aligns with the *Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers (May 2024)*.

This policy outlines our approach to data sharing, information sharing, and record keeping, ensuring that personal information is collected, stored, and shared appropriately, with due consideration to confidentiality, safeguarding, and legal obligations.

---

1. Aims of the Policy

- To ensure that all data sharing, information sharing, and record-keeping practices comply with GDPR and the Data Protection Act 2018.
- To promote the appropriate and timely sharing of information in line with safeguarding responsibilities, referencing the *Information Sharing: Advice for Practitioners* (2024).
- To protect the privacy, confidentiality, and security of personal data for children, families, and staff.
- To outline the procedures for securely collecting, storing, and sharing personal data within the setting and with external agencies.

---

2. Key Principles of GDPR (General Data Protection Regulation)

GDPR requires that personal data is:

- **Processed lawfully, fairly, and transparently:** We will only collect and process data with valid consent, legal obligation, or for the vital interests of the individual.
- **Collected for specific, explicit, and legitimate purposes:** Data will only be used for the purposes for which it was collected.
- **Minimised:** We will only collect the data necessary for the purpose.
- **Accurate and kept up-to-date:** We will ensure that personal data is accurate and updated as necessary.
- **Stored securely:** Appropriate measures will be in place to prevent unauthorised access or loss of data.
- **Kept no longer than necessary:** Data will be retained in line with our data retention policy and securely disposed of when no longer required.

3. Types of Information Collected

We collect and hold a range of personal data, including:

- **Children's Information:** Names, dates of birth, addresses, health and medical information, special educational needs, attendance records, and safeguarding concerns.
- **Parents/Carers' Information:** Contact details, family circumstances, and relevant consents for the care of the child.
- **Staff Information:** Personal details, employment history, performance records, DBS checks, and any relevant safeguarding concerns.
- **Safeguarding Information:** Sensitive information related to safeguarding concerns, disclosures, and reports to external agencies.

---

4. Lawful Bases for Processing Personal Data

Under GDPR, we ensure that personal data is processed based on one or more of the following lawful bases:

- **Consent:** Where explicit consent has been obtained from the individual (or parent/carer for children) to collect and process their data.
- **Contractual Obligation:** Where processing is necessary to fulfil the terms of a contract (e.g., employment contracts).
- **Legal Obligation:** Where processing is required to comply with the law (e.g., safeguarding regulations, health and safety requirements).
- **Vital Interests:** Where processing is necessary to protect the vital interests of the individual or another person (e.g., in an emergency).
- **Public Task:** Where processing is necessary to carry out a task in the public interest (e.g., provision of early years education).
- **Legitimate Interests:** Where processing is in the legitimate interests of the setting, provided that this does not override the rights and freedoms of the individual.

---

5. Information Sharing

Importance of Information Sharing
Effective information sharing is essential for promoting the welfare and protection of children. In line with the *Information Sharing: Advice for Practitioners* (May 2024), we will share information with other practitioners, agencies, and authorities where it is necessary to protect children and ensure their well-being.

Principles of Information Sharing
We follow the key principles outlined in the *Information Sharing: Advice for Practitioners* (2024):

- **Necessary and Proportionate:** We will only share information that is relevant and necessary to achieve the intended purpose.
- **Relevant:** Information shared will be directly related to the issue being addressed.

- **Adequate and Accurate:** We ensure that the information is accurate, up-to-date, and shared in an appropriate manner.
- **Timely:** Information will be shared in a timely manner to ensure effective action can be taken.
- **Secure:** Information will be shared securely, and measures will be in place to protect the confidentiality of those involved.
- **Accountable:** Decisions to share information will be documented, including the rationale for sharing and with whom it was shared.

When We Will Share Information
We will share information in the following circumstances:

- **Safeguarding:** When there are concerns about a child's welfare or safety, information may be shared with relevant external agencies (e.g., social services, the police, Local Authority Designated Officer (LADO)) without consent if it is in the best interests of the child.
- **Health and Safety:** Sharing information to protect individuals from harm or to manage medical conditions (e.g., sharing with healthcare providers).
- **Transitioning to Schools/Other Settings:** With parental consent, information may be shared with schools or other educational settings to support the child's transition.
- **Legal Requirements:** When required by law (e.g., inspections by Ofsted, legal investigations), we will share information with the relevant authorities.
- **General Running of the Nursery:** We have contracts with Parenta Database and Parental Portal for invoicing and communication with parents, Accountants, DBS requests, SES security, Insurance, Training Providers.

Gaining Consent
In most cases, we will seek consent from parents/carers before sharing personal information. However, consent may not be sought if it is deemed that seeking consent could place a child at greater risk (e.g., in safeguarding cases). When consent is obtained, parents/carers will be informed about what information will be shared, with whom, and for what purpose.

---

6. Information Sharing in the Context of Safeguarding

Importance of Information Sharing
Effective information sharing is essential for keeping children safe. In line with the *Information Sharing: Advice for Practitioners Providing Safeguarding Services* (May 2024), we recognise that sharing information in a timely manner can help prevent harm to children.

Key Principles of Information Sharing
When sharing information:

1. **Necessary and Proportionate:** Only share information that is necessary for the purpose it is being shared.
2. **Relevant:** Ensure the information shared is relevant and fits the context of the concern.

3. **Adequate:** Share enough information to address the concern, but no more.
4. **Accurate:** Ensure the information is accurate and up-to-date.
5. **Timely:** Information should be shared in a timely manner to prevent harm or support the child's welfare.
6. **Secure:** Data should be shared securely to protect confidentiality.
7. **Record:** Document decisions around information sharing, including what was shared, with whom, and for what purpose.

Safeguarding and Child Protection

- In cases where there are safeguarding concerns, information may be shared without consent if it is believed that obtaining consent would place a child at risk of harm.
- We will follow local safeguarding procedures and work closely with multi-agency partners, such as social services or the police, to share relevant information when necessary.
- Staff will receive regular training on how to identify safeguarding concerns and when and how to share information appropriately.

---

7. Record Keeping

Types of Records Kept
We maintain a variety of records, including:

- **Children's Records:** Personal information, registration details, medical records, development assessments, and safeguarding information.
- **Staff Records:** Personal information, employment contracts, training records, and DBS checks.
- **Attendance Records:** Daily registers for children and staff.
- **Accident and Incident Records:** Reports of any accidents or incidents occurring within the setting.
- **Safeguarding Records:** Detailed logs of any safeguarding concerns, disclosures, or referrals to external agencies.

Secure Storage of Records

- Records will be stored securely in locked cabinets for paper records or password-protected digital systems for electronic records. Electronic files are stored within Abacus, Dayshare and Footsteps, as controlled by the Parenta Group who are our external processors. Nursery computers are kept secure with appropriate software to ensure maximum protection against ransom and malware which is regularly updated.
- Access to records will be restricted to authorised staff members who require the information to perform their duties.
- Personal data will not be kept for longer than necessary and will be securely disposed of in accordance with Record Keeping legislation.
- Paper records will be stored in a waterproof location, and not in cardboard boxes or on ground level to avoid the risk of flooding.

Retention of Records
We will retain personal records in line with statutory requirements, following the EYA Retention Records (see S4.3 A Practical Guide to Record Keeping and Retention Periods). Examples of retained records include:

Attendance registers, Parental permission forms, medication records, SEND files, Safeguarding information.

---

8. Data Security

Protection of Data
We will implement appropriate security measures to protect personal data from unauthorised access, loss, or damage. These include:

- Password-protected systems for digital records.
- Locked cabinets for paper records.
- Restricted access to sensitive data, only available to authorised personnel.

Data Breaches
In the event of a data breach, we will follow the following procedures:

- Assess the extent and nature of the breach.
- Report significant breaches to the Information Commissioner's Office (ICO) within 72 hours, as required by GDPR.
- Inform individuals affected by the breach, where appropriate.
- Implement measures to mitigate the impact of the breach and prevent future occurrences.

---

9. Rights of Individuals

Under GDPR, individuals have the following rights regarding their personal data:

- **Right to Access:** Individuals (or parents/carers on behalf of their children) can request access to their personal data.
- **Right to Rectification:** Individuals can request that inaccurate or incomplete data be corrected.
- **Right to Erasure:** Individuals can request that their personal data be erased, subject to certain conditions.
- **Right to Restrict Processing:** Individuals can request that the processing of their data be restricted under specific circumstances.
- **Right to Object:** Individuals have the right to object to the processing of their personal data in certain situations.

Requests to exercise any of these rights should be made in writing to Chantelle Matts, the setting's Data Protection Officer (DPO).

10. Confidentiality

- All staff, volunteers, and visitors must maintain confidentiality in line with the setting's Confidentiality Policy.
- Personal data and information will only be shared on a need-to-know basis.
- Staff are required to sign a confidentiality agreement, acknowledging their responsibilities under GDPR and the Data Protection Act.

---

11. Staff Training

- All staff will receive training on GDPR, data protection, and information sharing as part of their induction and ongoing professional development.
- Staff will be trained on how to handle sensitive information, share data securely, and follow safeguarding procedures when sharing information.

Cross-Reference with: S1.3 Safer Recruitment Policy and Procedure S2.1 Admissions Policy and Procedure S4.1 Confidentiality Policy and Procedure S6.1 Accident and Incident Reporting S10.1 SEND Policy and Procedure S12.2 Partnership with Parents S13.1 Safeguarding Policy and Procedure S13.2 Child Protection Policy and Procedure Appendix - Record Keeping and Retention Periods	**Date of Review:** 01.11.25 **Next Review Due:** 01.11.26 **Approved by:** KMT

OPERATIONAL PLAN STANDARD 4 - CONFIDENTIALITY AND RECORD-KEEPING
Supporting Documentation S4.2 GDPR and Record Keeping Policy and Procedure

Record Keeping and Retention Periods – Practical Guide for Early Years Settings

(Based on current UK legislation, the Data Protection Act 2018, EYFS 2024/25, and local authority guidance)

Record Type	Retention Period	Reason / Legal Reference
Child's individual file / registration forms	Until child reaches **21 years + 3 months** (or 24 years + 3 months if child protection concerns)	Limitation Act 1980 – potential claims for negligence
Accident and incident records (child)	21 years + 3 months	Limitation Act 1980
Accident records (staff or visitor)	7 years from date of incident	Health & Safety Regulations
Medication records / administration forms	21 years + 3 months	Limitation Act 1980 – health record of a child
Child protection records	Until child reaches **24 years + 3 months**	Local Safeguarding Partnership guidance
Children's attendance registers	3 years from last entry	EYFS 3.77; Ofsted evidence requirement
Daily registers (staff rotas / deployment)	3 years	Working Time Regulations 1998

Learning and development records (learning journeys)	Return to parents when child leaves or destroy after 3 years	Good practice / data minimisation
Two-year progress checks	Keep with child's file (21 yrs + 3 m) if retained	EYFS requirement
SEND support plans / SEN referrals	21 years + 3 months	Limitation Act 1980
Parental consents / permissions (photos, outings, medication, etc.)	3 years after child leaves	EYFS & GDPR accountability
Financial records (fees, invoices, accounts)	6 years	HMRC requirement
Funding and census data (e.g. EYE funding forms)	6 years	Local authority audit requirement
Recruitment records – unsuccessful applicants	6 months – 1 year	Data Protection Act 2018
Staff personnel files / training records	6 years after employment ends	Employment Rights Act 1996
DBS checks / references (evidence only, not certificate)	Keep evidence of check date & reference – delete certificate info immediately after verification	DBS Code of Practice

Staff accident / injury records	7 years	RIDDOR 1995
Health and safety checks / risk assessments	3 years	Health & Safety Regulations
Fire drill and equipment test logs	3 years	Fire Safety Order 2005
Food safety / kitchen records	3 years	Food Standards Agency – Food Hygiene Regs
Visitor sign-in records	3 years	Security and safeguarding evidence
Complaints records (EYFS)	3 years after complaint resolved	EYFS 3.77
Accreditation / inspection evidence	Until next inspection + 3 years	Ofsted / LA verification
CCTV footage (if applicable)	28 days maximum unless required for investigation	ICO CCTV Code of Practice