Data Protection, Confidentiality, Information Sharing and CCTV Policy

At Incey Winceys Day Nursery and Preschool, we are committed to protecting personal data and maintaining confidentiality in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Early Years Foundation Stage (EYFS) 2026 statutory framework. This policy outlines how we collect, store, share, and protect personal information about children, parents, carers, and staff, ensuring we meet our legal and ethical obligations.

1. Data Protection and Children's Records

We maintain accurate and secure records to support each child's care, learning and development, and to comply with statutory and regulatory requirements. All personal data is processed fairly, lawfully and transparently, with appropriate security measures in place.

We hold two categories of records:

- Developmental Records – including observations, assessments, photographs, and reports. These are stored securely on password-protected systems accessible only to authorised staff and parents via secure logins.
- Personal Records – including registration forms, consent forms, correspondence, safeguarding information, and meeting notes. These are stored in a locked office and/or secure digital storage, accessible only to management and relevant staff on a need-to-know basis.

All records are retained according to our data retention schedule and securely destroyed when no longer required. Information is shared with other settings or professionals only where it is lawful, necessary, and in the best interests of the child.

Revised 9th October 2026

2. Confidentiality and Client Access to Records

We respect the privacy of children and their families. Information shared with us is treated as confidential and used only to support the child's welfare, safety, and learning. We ensure parents and carers can share information in confidence, knowing that it will be handled appropriately and lawfully.

Confidentiality procedures include:

- Gaining consent from parents to share developmental information with local authorities or support agencies where appropriate.
- Ensuring all records are kept secure and shared only with authorised persons.
- Informing parents if confidential records need to be kept regarding injuries, concerns, or safeguarding issues.
- Providing access to their own child's records upon written request, in line with the UK GDPR Right of Access.

3. Information Sharing

We recognise that information sharing is essential for effective safeguarding and promoting the welfare of children. The EYFS 2026 framework reinforces that practitioners must share relevant information with agencies involved in safeguarding and child protection, even without consent where necessary to protect a child from harm.

We will share information when:

- It is required by law or regulation.
- It is necessary to protect a child from harm or to prevent a crime.
- It is in the public interest and proportionate to the purpose.
- It supports effective transitions or the continuity of care between settings.
  All staff understand that safeguarding obligations override data protection restrictions. Decisions to share information without consent are made with management oversight and recorded in the child's confidential record.

Revised 9th October 2026

4. CCTV and Data Security

The nursery uses CCTV for the purposes of safeguarding, security, and monitoring interactions to improve the quality of care. All CCTV use complies with the Data Protection Act 2018 and UK GDPR principles.

- Cameras cover entrances, play areas, and staff areas but never toilets or changing areas.
- CCTV footage is recorded without sound and retained for up to six weeks before secure deletion.
- Footage is accessed only by management and may be shared with the police or safeguarding authorities where a lawful basis exists.
- Parents do not have access to CCTV footage to protect the privacy of all children.

5. Data Retention and Security Measures

All records are maintained in accordance with our retention schedule and securely destroyed when no longer required. Examples include:
• Safeguarding records – retained until the child reaches 25 years old.
• Attendance and accident records – retained for 6 years.
• Financial and business records – retained for 7 years.
We implement strict data security measures including password protection, encrypted devices, restricted access, and regular staff training. Paper records are stored in cabinets and digital records on secure systems with access logs.

6. Staff Responsibilities and Training

All staff are responsible for maintaining confidentiality and protecting data. Induction and ongoing training cover data protection principles, safe information sharing, and EYFS 2026 safeguarding updates. Staff must not discuss confidential information outside the nursery or with unauthorised persons.

Revised 9th October 2026

Breaches of data protection or confidentiality may result in disciplinary action and must be reported immediately to management for investigation and notification to the ICO if required.

7. EYFS 2026 Safeguarding and Welfare Updates

This policy incorporates EYFS 2026 safeguarding and welfare requirements, including:

- Maintaining a minimum of two emergency contacts per child and verifying contact details regularly.
- Strengthened absence monitoring to follow up unexplained absences promptly.
- Clear whistleblowing and safer recruitment procedures.
- Safer eating practices and recording of incidents.
- Privacy and supervision balance during intimate care routines.

All staff must be aware of these updates and apply them consistently in daily practice.

8. Monitoring and Review

This policy is reviewed annually, or sooner if there are changes in legislation, EYFS guidance, or data protection practices. The Data Protection Lead is responsible for overseeing compliance, responding to subject access requests, and ensuring that all staff follow this policy.