



Data Protection and Confidentiality Policy

Updated in line with UK GDPR, the Data Protection Act 2018 as amended, the Data (Use and Access) Act 2025, EYFS effective 1 September 2026, Working Together to Safeguard Children 2026, and KCSIE 2026 as supplementary safeguarding guidance.

At Ringle Rainbow Nursery, we are committed to protecting the confidentiality, privacy and personal information of children, families, staff and others connected with the nursery. Personal data will be processed lawfully, fairly and transparently, collected for specified purposes, limited to what is necessary, kept accurate, retained only for as long as required and protected by appropriate organisational and technical measures.

Responsibilities

Penny Reidy is the named Data Protection Lead and is responsible for overseeing data-protection compliance, privacy information, data-rights requests, data breaches, complaints and appropriate risk assessments. All staff are responsible for maintaining confidentiality and handling information securely and receive relevant training during induction and through ongoing updates.

Legal and Safeguarding Framework

The nursery processes personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 as amended by subsequent legislation including the Data (Use and Access) Act 2025, and other applicable data-protection law. The nursery also follows the EYFS statutory framework effective 1 September 2026 and Working Together to Safeguard Children 2026. Keeping Children Safe in Education (KCSIE) 2026 is used as supplementary safeguarding good-practice guidance.

Data protection law does not prevent appropriate information sharing to safeguard a child. Staff must be proactive in sharing relevant information where this is necessary and proportionate to identify, assess or respond to risks to a child's safety or welfare. Consent is not required where another lawful basis permits or requires safeguarding information to be shared.

Personal Information We Collect

The nursery may process names, addresses and contact details; emergency contacts; dates of birth; attendance; photographs; learning and development records; funding information; medical, allergy and dietary information; SEND information; accident and medication records; safeguarding information; and staff employment and suitability information. Health, safeguarding and certain other information may be special-category data and will receive additional protection.



Lawful Bases and Transparency

Personal data will only be processed where an appropriate lawful basis applies. Depending on the purpose, this may include legal obligation, contract, legitimate interests, vital interests, public task or consent. Where special-category data is processed, an additional condition under data-protection law will also be identified. Appropriate privacy information will explain how and why data is used, shared and retained and the rights available to individuals.

Use of BabysDays

Ringle Rainbow Nursery uses BabysDays as its nursery management system to record and manage information including attendance, learning observations, medical and medication records, accident information and other approved records. Access is restricted to authorised users and staff must follow secure password and access-control procedures. Third-party processors will be appropriately assessed and governed by suitable data-processing arrangements.

Use of Artificial Intelligence (AI)

AI-enabled functions may be used for approved administrative or operational purposes where appropriately assessed, for example reminders, reporting assistance, trend identification or routine record-keeping support. All AI-generated content or insights must receive meaningful human review. AI must not replace professional judgement or make solely automated safeguarding, health, welfare or behaviour decisions about a child with legal or similarly significant effects without an appropriate lawful basis and safeguards.

Staff must not enter personal, special-category, confidential or safeguarding information about children, families or colleagues into unapproved external AI services. Any new AI service or significant AI function must be authorised by the Nursery Manager/Data Protection Lead and assessed for privacy, security and safeguarding risks. A Data Protection Impact Assessment (DPIA) will be completed where required.

Data Protection Impact Assessments and New Technology

A DPIA will be considered before introducing processing likely to result in a high risk to individuals' rights and freedoms, including certain uses of AI, profiling, biometric technology, extensive monitoring or new systems processing sensitive information. Identified risks will be reduced before processing begins wherever possible.

Individual Data Rights

Individuals have rights which may include access, rectification, erasure, restriction, data portability, objection and rights relating to automated decision-making. These rights are not absolute and depend on the circumstances and lawful basis. Requests should be directed to the Nursery Manager or Data Protection Lead and will be handled within the applicable statutory timescale.



Sharing and Confidentiality

Personal information will only be shared where there is an appropriate lawful basis and the sharing is necessary and proportionate. This may include the local authority, Ofsted, health professionals, social care, police, funding bodies or other agencies. Safeguarding information will be shared in accordance with Working Together to Safeguard Children 2026 and applicable information-sharing requirements. Staff should record significant safeguarding information-sharing decisions, including what was shared, with whom and why.

Security and Access

Paper and digital records will be stored securely with access limited to authorised people. Staff must not share passwords, leave confidential information accessible, or copy personal data to personal devices, personal email, unauthorised cloud storage or unapproved apps. Confidential conversations will take place discreetly.

Retention and Secure Disposal

Records will be retained in accordance with legal, regulatory, safeguarding, insurance and operational requirements and will not be kept for longer than necessary. When records are no longer required, paper and electronic information will be securely destroyed or deleted.

Data Breaches

Any suspected loss, unauthorised disclosure, alteration, destruction or access to personal data must be reported immediately to the Data Protection Lead. The nursery will investigate and record breaches, contain and reduce harm, and assess notification requirements. Where a breach is likely to result in a risk to individuals' rights and freedoms, the ICO will be notified without undue delay and, where feasible, within 72 hours of awareness. Where a high risk is likely, affected individuals will also be informed without undue delay unless an applicable exception applies.

Data Protection Complaints

Individuals may complain about how their personal data has been processed. Complaints may be made verbally or in writing to the Nursery Manager or Data Protection Lead. The nursery will provide an accessible route for complaints, acknowledge a data-protection complaint within 30 days, take appropriate steps to investigate it without undue delay, keep the complainant appropriately informed and communicate the outcome. Individuals may also raise concerns with the Information Commissioner's Office.

Staff Conduct and Confidentiality

Staff must maintain professional confidentiality during and after employment. Information obtained through work must not be discussed socially, posted online or disclosed to unauthorised people. Deliberate or negligent breaches may result in disciplinary action and, where appropriate, referral to relevant authorities.



Monitoring and Review

The Data Protection Lead will keep this policy and the nursery's data-handling arrangements under review, including changes to legislation, ICO guidance, safeguarding information-sharing requirements and technology used by the setting.

Policy Date: 01/09/2026

Review Date: 01/09/2027

By: P Reidy