Data Protection Policy

Grass Roots Nursery Group

Updated September 2026

1. Purpose & Scope

The purpose of this policy is to establish formal procedures for the collection, handling, processing, and secure storage of personal data at Grass Roots Nursery Group. This policy ensures full compliance with UK data protection laws while proactively protecting the rights and privacy of children, parents, employees, and visitors across all setting sites.

Scope:

This policy applies to all employees, volunteers, students, contractors, and third-party suppliers associated with Grass Roots Nursery Group.

2. Statutory Framework & Reference Guidance

This policy operates in full compliance with:

- Data (Use and Access) Act 2025
- Data Protection Act 2018 & UK GDPR
- Early Years Foundation Stage (EYFS) Statutory Framework (2026)
- Keeping Children Safe in Education (KCSIE, 2026)
- Children's Wellbeing and Schools Bill 2025

3. Core Data Protection Principles

Grass Roots Nursery Group adheres strictly to the seven UK GDPR principles:

- **Lawfulness, Fairness & Transparency**
- **Purpose Limitation**
- **Data Minimisation**
- **Accuracy**
- **Storage Limitation**
- **Integrity & Confidentiality**
- **Accountability**

Leadership maintains documented evidence demonstrating full compliance with these principles.

4. Operational Guidelines for Digital Platforms & Security

Digital Management Systems

Famly Platform:

Daily observations, attendance, meal tracking, and parent communications are processed via Famly. Access is strictly role-restricted and password-protected.

CPOMS Safeguarding Portal:

Sensitive child protection notes, unwitnessed injury logs, and multi-agency referrals are stored securely on CPOMS. Access is restricted to the Designated Safeguarding Lead (Emma Ford) and nursery leadership.

Funding Loop Declarations:

Parent funding claims submitted for Calderdale local authority funding are processed via the secure Funding Loop platform under encrypted standards. Only authorised staff may submit claims.

Google Drive Infrastructure:

Contracts, personnel files, HR records, and financial documents are stored on setting Google Drive accounts secured by mandatory Two-Factor Authentication (2FA).

Technical Hygiene & Hardware Governance

Nursery Hardware Only:

- Child or operational data must only be accessed using nursery-owned, password-protected tablets and laptops. Personal devices are strictly prohibited.

Password Standards & MFA:

- Passwords must follow the "Three Random Words" passphrase model. Multi-Factor Authentication (MFA) is mandatory for all administrative and safeguarding accounts.

Clean Screen Standard:

- When displaying records or photos to parents, staff must suppress notification pop-ups and hide other children's personal information.

Generative AI Rules:

- Staff using AI tools (e.g., Google Gemini) must use official Google Workspace accounts and must not enter identifiable child, parent, or staff data. AI outputs must be checked for accuracy before use.

DBS Identity Evidence & Safe Recruitment Storage

Grass Roots Nursery Group retains copies of identity documents used to verify an applicant's identity for DBS checks, in line with KCSIE safe recruitment guidance.

Secure Handling:

Digital copies are encrypted and stored in restricted-access personnel folders on Google Drive (2FA protected).

- Physical copies are locked securely in management personnel files.

Access & Retention:

Access is restricted to Directors and the Safe Recruitment Lead.

- Evidence is retained for the duration of employment/placement and securely erased upon termination.

Staff HR Records

Personnel files include:

- medical information
- emergency contact details
- training records
- appraisal and supervision notes
- disciplinary records

These are stored securely on Google Drive with restricted access and retained in line with statutory HR retention schedules.

5. Individual Rights & Subject Access Requests (SARs)

Grass Roots Nursery Group respects the statutory rights of individuals regarding their personal information.

Right to Information:

- Transparent privacy notices are provided to staff and families.

Subject Access Requests (SARs):

- Requests are fulfilled within 30 calendar days, free of charge.

“Stop the Clock” Provision (2025 Act):

- The nursery may pause the 30-day deadline if clarification or identification is required.

Internal Complaint Rights:

- Individuals may raise data-handling concerns directly with setting leadership before escalating to the ICO.

Rectification & Erasure:

- Individuals may request correction of inaccurate data or erasure where retention is no longer legally required.

6. Photography, Images & Video

- Images and videos are captured only on nursery-owned devices.
- Parent consent is required for all non-essential photography.
- Images are uploaded to Famly and not stored on personal devices.
- Photos and videos are deleted annually as part of data-weeding procedures.

7. Disclosure, Retention & Data Weeding

Law Enforcement Disclosures:

- Personal data is disclosed only when legally required or necessary for safeguarding. All requests are vetted by management.

Data Weeding & Retention Schedules:

Management conducts regular audits to securely destroy records that have passed statutory retention limits.

- Paper records are cross-shredded; digital files are permanently erased.

DBS Verification Evidence:

- Identity evidence is retained securely for the duration of employment and erased upon termination.

8. Breach Response & ICO Reporting

If a personal data breach, security leak, or cyber incident occurs:

Immediate Containment:

1. Disconnect affected devices from Wi-Fi/Ethernet and notify the Nursery Manager or DPO immediately.

Investigation:

Management assesses the scope, risk level, and nature of compromised data.

2. Staff must not attempt to investigate breaches independently.

72-Hour ICO Notification:

3. Any breach posing a risk to individuals’ rights or freedoms will be reported to the ICO within 72 hours.

9. Roles, Training & Policy Governance

Data Protection Officer (DPO):

- **Lucy Pottinger** — responsible for overseeing compliance and responding to data concerns.

Leadership:

- Holds ultimate accountability for regulatory compliance.

Designated Safeguarding Lead (Emma Ford):

- Manages safeguarding data integrity within CPOMS and liaises with statutory bodies.

All Staff:

- Must follow data hygiene protocols, password standards, privacy guidelines, and breach reporting procedures.

Annual Training:

- All staff receive annual data protection training covering secure handling, digital hygiene, and breach response.