Online Safety & Acceptable Use Policy

Grass Roots Nursery Group
Updated September 2026

1. Policy Statement

Grass Roots Nursery Group is committed to ensuring the safe, responsible, and developmentally appropriate use of technology across all settings. Online safety is an essential part of safeguarding. We protect children from digital harm, support staff in maintaining professional online boundaries, and ensure that all digital systems, devices, and platforms are used securely and lawfully.

Children do not use internet-enabled devices in the setting. Staff model safe, professional behaviour at all times and follow strict protocols for device use, data protection, filtering and monitoring, digital communication, and AI use.

This policy works alongside our Safer Internet Use, Data Protection, Cyber Security Essentials, Mobile Phone & Electronic Device Use, AI Acceptable Use, and Safeguarding policies.

2. Purpose & Scope

This policy outlines how Grass Roots Nursery Group manages online safety, digital safeguarding, acceptable internet use, and AI use across all settings. It ensures:

- children are protected from digital risks
- staff use technology safely and professionally
- personal data is handled securely
- filtering and monitoring systems meet statutory standards
- online safety incidents are logged and escalated appropriately
- digital images are captured and stored securely
- AI tools are used safely and lawfully
- parents receive consistent online safety guidance

This policy applies to:

- employees
- apprentices and students
- volunteers
- agency staff
- contractors
- visitors using nursery devices or networks

It covers:

- internet access
- digital images and storage
- staff personal devices
- nursery-owned hardware
- online platforms (Famly, Google Workspace, Funding Loop, CPOMS)
- filtering and monitoring
- AI use (Gemini, Famly AI tools)
- incident reporting and escalation

3. Statutory Framework & Reference Guidance

This policy operates in full compliance with:

- Working Together to Safeguard Children (2026)
- Keeping Children Safe in Education (2026) – Filtering & Monitoring Standards
- Early Years Foundation Stage (2026)
- Online Safety Act (2023)
- Data Protection Act (2018)
- UK GDPR
- Data (Use and Access) Act (2025)
- National Cyber Security Centre (NCSC) Guidance
- Calderdale Safeguarding Children Partnership Procedures
- West Yorkshire Consortium Inter-Agency Safeguarding Procedures

Linked internal policies include:

- Data Protection Policy
- Cyber Security Essentials Policy
- Mobile Phone & Electronic Device Use Policy
- AI Acceptable Use Policy
- Safeguarding & Child Protection Policy
- Allegations Against Staff Policy
- Whistleblowing Policy
- Staff Code of Conduct

4. Online Safety & Acceptable Use Procedures

A. Leadership & Governance Responsibilities

- The DSL (Emma Ford) and leadership team conduct annual reviews of filtering and monitoring systems across all sites.
- Filtering systems must meet KCSIE 2026 standards and prevent access to harmful content.
- SWGfL test lines are used termly to verify filtering effectiveness.
- Evidence of filtering checks is stored on BrightSafe.
- Staff receive mandatory training in online safety, data protection, cybersecurity, and AI use.
- All digital systems (Famly, Google Workspace, CPOMS) must use Two-Factor Authentication (2FA).

B. Technology Use with Children

- Children do not use tablets, smart speakers, or internet-enabled devices in the setting.
- Smart speakers are prohibited in children's rooms due to risks of voice recording and data capture.
- Any digital content shared with children (e.g., photos, videos) is supervised and purposeful.
- Children are never given unsupervised access to the internet.
- Early digital awareness is taught through simple, age-appropriate safety messages such as:
    - "We ask a grown-up for help."
    - "We only use technology with a teacher."
    - "If something feels yucky or strange, we tell an adult."

C. Staff Personal Devices & Mobile Phones

- Personal mobile phones, smartwatches, and personal electronic devices must be switched off/silenced and stored in designated lockers in the office.
- Personal devices must never be used to photograph, record, or communicate about children.
- Staff must not access Famly, CPOMS, or Google Workspace on personal devices.
- All communication with families must take place via nursery-owned hardware and official accounts.

D. Nursery-Owned Hardware & Digital Images

- Observations and photos are captured only on nursery-owned, password-protected tablets.
- Images are stored securely on Google Workspace (2FA enabled) and uploaded to Famly.
- Practitioners must follow Clean Screen hygiene when sharing devices with parents.
- No images may be stored on personal devices or transferred outside secure systems.
- Parental consent must be checked before capturing images.
- Images are moderated by management before sharing.
- Images are deleted in line with the Data Protection Policy and retention schedule.

E. Online Platforms & Apps (Famly, CPOMS, Google Workspace)

- Famly is the secure platform for learning journeys, daily logs, and parent communication.
- Access is role-restricted and password-protected.
- Staff must follow data protection expectations when uploading or sharing information.
- CPOMS is used for safeguarding concerns, filtering bypasses, and digital incidents.
- Parents are reminded not to screenshot or share images of other children on social media.

F. Artificial Intelligence (AI) Acceptable Use

Famly AI (Internal / Secure AI)

- May be used to refine observations, suggest next steps, or generate activity ideas.
- Staff must verify accuracy before publishing.
- AI suggestions must be personalised to the child.

Google Gemini (Creative / Admin AI)

- May be used for lesson planning, newsletters, policy drafting, and activity ideas.
- **The No-Name Rule:** Staff must never input identifiable child, family, or staff data.
- Allowed: “Give me sensory play ideas for 2-year-olds.”
- Prohibited: “Write a report for [Child Name].”

Prohibited AI Actions

- No deepfakes or synthetic media involving children.
- No uploading images of children into AI tools.
- No personal AI accounts for nursery work.
- No AI-generated risk assessments — human judgement is required.

AI Data Breach Protocol

- If sensitive data is accidentally entered into Gemini, staff must inform the Nursery Manager immediately for a risk assessment.

G. Handling Online Safety Incidents

Examples include:

- unexpected pop-ups
- filtering bypass attempts
- suspicious emails
- phishing attempts
- malware warnings
- staff misuse

Reporting routes:

- **Safeguarding concerns → CPOMS**
- **Operational breaches → BrightSafe**
- **Cyber incidents → Nursery Manager + DSL**
- **Serious breaches → ICO within 72 hours**
- **Illegal content → Police (999 if immediate danger)**

H. Child-Friendly Online Safety Messages

Practitioners reinforce simple, age-appropriate safety principles:

- "We always ask a grown-up for help with technology."
- "We only use technology with a teacher."
- "If something makes us feel unsure, we tell an adult."
- "We keep ourselves safe by staying close to our grown-ups."

5. Monitoring & Review

This policy is reviewed annually or sooner if legislation, technology, or emerging risks change. DSLs oversee implementation across all settings.

6. Linked Policies

- Safeguarding & Child Protection Policy
- Mobile Phone & Electronic Device Use Policy
- Data Protection Policy
- Cyber Security Essentials Policy
- Allegations Against Staff Policy
- Whistleblowing Policy
- Staff Code of Conduct
- AI Acceptable Use Policy
- Premises Security Procedures

Appendix 1

E-Safety Incident Log

Date of Incident	Name of individuals involved	Device Location	Details of Incident	Actions and Reasons	Confirmed by