Cyber Security Essentials Policy

Grass Roots Nursery Group

Updated September 2026

1. Policy Statement

Grass Roots Nursery Group is committed to protecting the confidentiality, integrity, and availability of all digital systems, electronic data, and IT infrastructure across all settings. Cyber security is a core safeguarding responsibility. We manage sensitive child protection records, personal data, financial information, and operational systems that require robust digital protection.

This policy sets out mandatory cyber security standards for all staff, students, volunteers, and contractors to prevent data breaches, unauthorised access, phishing, ransomware, and digital misuse.

2. Purpose & Scope

This policy ensures:

- secure use of nursery digital systems
- protection of child, family, and staff data
- compliance with statutory filtering & monitoring standards
- safe use of AI tools
- secure device management
- clear cyber incident response procedures

It applies to:

- all employees
- apprentices and students
- volunteers
- agency staff
- contractors
- any adult accessing nursery digital systems or networks

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)
- Data Protection Act (2018)
- UK GDPR
- Data (Use and Access) Act (2025)
- National Cyber Security Centre (NCSC) Guidance
- Calderdale Safeguarding Children Partnership Procedures (current)

4. Cyber Security Procedures

A. Network Security

- All nursery networks use secure, encrypted Wi-Fi.
- Guest Wi-Fi is separated from staff networks and cannot access nursery systems.
- Firewalls and router security settings are reviewed annually.
- Only authorised nursery devices may connect to nursery networks.

- Network passwords are changed annually or immediately following a breach.

B. Filtering & Monitoring (KCSIE 2026)

Grass Roots meets statutory filtering and monitoring standards:

- Internet filtering blocks harmful or inappropriate content.
- Monitoring systems flag suspicious activity or filtering bypass attempts.
- DSL (Emma Ford) and leadership conduct annual filtering reviews and store evidence on BrightSafe.
- Filtering systems are tested termly using SWGfL test lines.
- Any unexpected pop-up or bypass is logged on CPOMS and investigated immediately.

C. Device Security & Hardware Governance

- **Nursery-owned hardware only** may be used for Famly, CPOMS, Funding Loop, Google Workspace.
- Personal devices must never access nursery systems.
- **2-minute screen lock rule** applies to all nursery laptops, tablets, and desktops.
- Staff must manually lock screens when stepping away (Win+L or power button).
- All devices must use biometric locks or secure PINs.
- Device PINs/passwords must never be shared.
- Devices must not store data locally unless encrypted.
- Devices are securely wiped before disposal.

D. Password Integrity & Multi-Factor Authentication (MFA)

- Staff must maintain unique login credentials for all systems.
- Password sharing is strictly prohibited.
- MFA is mandatory for:
    - Google Workspace
    - CPOMS
    - Famly
    - Funding Loop
    - any admin/safeguarding accounts
- Passwords must follow the NCSC **Three Random Words** model.
- Passwords must never be written down or stored insecurely.

E. Access Control & Permissions

- Access to digital systems is strictly role-based.
- DSLs and leadership hold elevated safeguarding access.
- Staff receive only the minimum access required (“least privilege”).
- Access is removed immediately when staff leave or are suspended.
- Access logs are reviewed annually.

F. Safe AI, Internet & Network Usage

AI Use (Google Gemini)

- Staff must use only official Grass Roots Google Workspace accounts.
- **No identifiable child, family, or staff data** may be entered into AI tools.
- AI must never generate or alter images of children.
- Any accidental data entry into AI must be reported immediately.

Public Wi-Fi Prohibition

- Staff must not access nursery systems on public Wi-Fi.

- Off-site work must use secure home Wi-Fi or encrypted nursery hotspots.

Phishing & Link Vigilance

- Staff must not click unexpected links or attachments.
- Suspicious messages must be verified with the Manager before action.
- Staff must report phishing attempts immediately.

G. Staff Departures, Device Losses & Offboarding

- Lost or stolen nursery devices must be reported within **one hour**.
- Leadership will revoke credentials and remotely wipe devices.
- On a staff member's final day (or suspension), all access to nursery systems is revoked immediately.

H. Cyber Incident Response

If a cyber incident occurs:

- **Disconnect:** Turn off Wi-Fi or disconnect Ethernet immediately.
- **Report:**Notify the Nursery Manager or DSL.
- **Document:** Record exact details (time, link clicked, device used).
- **Investigate:**Leadership assesses risk and scope.
- **Statutory Reporting:** Breaches affecting personal data are reported to the ICO within **72 hours**. Safeguarding-related breaches may require MAST/LADO escalation.
- **Recovery:** Passwords reset. Devices patched or replaced. Staff retraining if human error contributed.

5. Monitoring & Review

This policy is reviewed annually or sooner if legislation, technology, or emerging risks change.
DSLs and leadership maintain evidence of filtering, monitoring, and cyber audits.

6. Linked Policies

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

Annual Filtering and Monitoring Review Log

Nursery Name: _____

Date of Review: _____

Review Lead (Name & Role): _____

Designated Safeguarding Lead (DSL): _____

IT Provider / Support Contact: _____

1. System Inventory & Infrastructure Scope

Verify that the review covers all entry points to the internet within the setting.

Infrastructure Category	**Covered? (Y/N)**	**Notes / Specific Software & Hardware Used**
Nursery Network / Wi-Fi		
Guest / Visitor Wi-Fi		
Staff Tablets & Devices *(e.g., for learning journals)*		
Office & Admin Desktops		
Smart Speakers / Displays *(e.g., Alexa, Google Nest)*		

2. Compliance & Effectiveness Assessment

A. Procurement & Provider Standards

- **Finding:** Does the filtering and monitoring provider meet the current DfE Digital and Technology Standards?
  `[ ] Yes [ ] No`
- **Evidence/Notes:**
  _____

B. Filtering Capabilities

- **Finding:** Are illegal, harmful, and age-inappropriate categories (including adult content and extremist material) effectively blocked?
  `[ ] Yes [ ] No`
- **Finding:** Are controls in place to block or manage unapproved Generative AI tools and chatbots?
  `[ ] Yes [ ] No`
- **Evidence/Notes:**
  _____

C. Monitoring & Safeguarding Alerts

- **Finding:** Does the system successfully generate alerts for high-risk activity, and do these route directly to the DSL team?
  `[ ] Yes [ ] No`
- **Finding:** Was a live drill or test of the alert escalation pathway completed during this review?
  `[ ] Yes [ ] No`
- **Evidence/Notes:**
  _____

D. Staff Training & Awareness

- **Finding:** Have all staff received training regarding their filtering and monitoring responsibilities and how to report system vulnerabilities?
  `[ ] Yes [ ] No`
- **Evidence/Notes:**
  _____

3. Identified Gaps & Required Actions

List any vulnerabilities, unmapped devices, or training gaps discovered during the review.

Ref	Identified Risk / Gap	Action Required	Responsible Person	Target Date	Status
1	*e.g., Guest Wi-Fi bypasses filter*	*Update router configuration with IT provider*	*J. Smith (IT)*	*DD/MM/YY*	*Pending*
2					
3					

4. Sign-Off & Approvals

By signing below, the nursery leadership confirms that the filtering and monitoring systems have been thoroughly tested, reviewed against statutory guidance, and that the action plan above will be monitored for completion.

Review Lead Signature: _____ Date: _____

Designated Safeguarding Lead Signature: _____ Date: _____

Proprietor / Director / Governor Signature: _____ Date: _____

Next Scheduled Review Date: _____