

Cyber Security Essentials Policy



Grass Roots Nursery Group: Cyber Security Essentials Policy

Device Security & Access

- **Authorised Devices Only:** Only nursery-owned tablets/laptops or manager-approved personal devices may be used to access **Famly** or the **Gemini** account.
- **The 2-Minute Rule:** All devices must have an automatic screen lock set to a maximum of 2 minutes of inactivity.
- **Biometrics/PINs:** Every device must be protected by a complex PIN. These must **never** be shared with parents or unauthorised visitors.

Password & Account Integrity

- **No Password Sharing:** Staff must never share their Famly login or the nursery's Google/Gemini credentials.
- **MFA (Multi-Factor Authentication):** Wherever possible (especially for the Manager's email and Famly admin accounts), MFA must be enabled (e.g., a code sent to a phone).
- **Strong Passwords:** Passwords should be "Passphrases"—three random, memorable words (e.g., **BlueTractorSowerby!**).

Safe AI & Web Usage (Gemini/Google)

- **Official Accounts Only:** Staff must only use the official Grass Roots Gemini account for work-related brainstorming.
- **Link Caution:** Do not click links in emails asking you to "re-verify" your Gemini or Famly password. Go directly to the app or website instead.
- **Public Wi-Fi:** Staff must not access Famly or nursery records using public, unencrypted Wi-Fi (e.g., in a coffee shop). Use the nursery's private Wi-Fi or a secure mobile hotspot.

Data Protection & "Phishing"

- **The "Pause" Rule:** If an email or message looks odd (even if it looks like it's from a parent or a supplier asking for a bank transfer or sensitive data), **stop** and check with the Manager in person before clicking.
- **Clean Feed:** When showing a parent something on a tablet in the nursery, ensure no other children's notifications or names pop up on the screen.

Staff Departures & Lost Devices

- **Immediate Reporting:** If a phone or tablet with nursery apps is lost or stolen, it must be reported to the Manager within **one hour** so accounts can be remotely locked.
- **Exit Protocol:** On a staff member's final day, all access to Famly, Gemini, and nursery emails will be revoked immediately.

Cyber Security Essentials Policy



Emergency "What If" Plan

If you think we have been hacked or data has been leaked:

1. **Disconnect:** Turn off the Wi-Fi on the affected device.
2. **Report:** Tell the Nursery Manager/Owner immediately.
3. **Document:** Note down what happened (e.g., "I clicked a link in an email that looked like it was from Family").