



Mobile & Remote Working Policy

Same risks, different locations. Simple rules for phones, laptops and working away from the office.

Work now happens on the move. This policy sets out how [Business name] keeps data safe on mobile devices and when staff work remotely.

Rules

- **Lock & encrypt.** Every device that touches work has a screen lock/PIN and full-disk encryption turned on.
- **Separate work.** Keep work on work accounts; don't store business data in personal cloud accounts.
- **Mobile hygiene.** Use MFA and the password manager on mobile too. Watch for scam texts (smishing) and fake apps.
- **Public Wi-Fi.** Avoid sensitive work on public Wi-Fi; use your phone's hotspot or a business-grade VPN.
- **Lost device.** Report a lost or stolen device immediately so access can be cut and the device wiped.

Policy owner: _____

Reviewed: _____

Make it yours (with AI)

I run a [type of business] in [town], Australia, with [number] staff. Rewrite the document below so it fits how my business works, in plain English my team will read. Keep it to one page. [paste the template]

Two rules: start a fresh chat, and never paste real customer names, bank details or staff records into a free AI tool.