



Acceptable Use Policy

How our devices, accounts and data may be used.

This policy sets out how staff and contractors at [Business name] may use our devices, accounts, internet and data.

Do

- Use your own individual login for everything, and lock your screen when you step away.
- Keep work on work accounts; keep automatic updates on.
- Use the company password manager and MFA.
- Report anything suspicious straight away — no blame for honest mistakes.

Don't

- Share passwords or accounts, or approve an MFA prompt you didn't start.
- Install unknown software, or plug in USB drives you don't trust.
- Forward work email to personal accounts, or store business data in personal cloud accounts.
- Pay or change bank details on the strength of an email alone (see the Payment policy).

Policy owner: _____

Staff member (name): _____

Signed / dated: _____

Make it yours (with AI)

I run a [type of business] in [town], Australia, with [number] staff. Rewrite the policy below so it fits how my business actually 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.