



AI Usage Policy

One-page version · SMB1001 Control 27 · From 'Shit, I've Been Hacked!'

AI tools are useful, but they carry real data-governance and security risks. This one-page policy keeps [Business name]'s use of AI simple, safe and proportionate.

Approved tools

[List your approved tools here — e.g. Claude Business, Microsoft Copilot, ChatGPT Team.] Anything outside this list requires a conversation before use.

What AI can be used for

Drafting documents and communications, summarising information, generating ideas, structuring notes and reports, research support.

What AI must not be used for

Approving payments or financial decisions, changing access credentials, sending unsupervised communications to clients or suppliers, or storing/processing customer personal information without checking your approved plan's data-handling terms.

What never goes into any AI tool

Passwords, MFA codes, tax file numbers, bank account details, customer personal records (in free or unmanaged tools), or confidential legal correspondence.

Before using a new AI tool

Check with [owner / manager] first.

If something goes wrong

Report it. No blame for honest mistakes, but we need to know.

Policy owner: _____

Reviewed (date): _____

Make it yours (with AI)

Rewrite the AI usage policy below for a [type of business] in Australia with [number] staff. Our approved tools are [list them]. The person staff check with is [role, not a name]. Keep it to one page, keep the plain English, and don't add anything we didn't ask for. [paste the policy]

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