

Team AI Usage Policy

A practical starter template — short enough that your team will actually read it. Replace every highlighted placeholder, delete what doesn't apply, and make it yours.

Organisation: [Your business name] Owner: [Name / role] Version: [1.0] Date: [dd/mm/yyyy]

How to use this template: anything in [gold brackets] is for you to fill in or decide.

1. Why we have this policy

AI tools like **Claude**, **ChatGPT** and **Microsoft 365 Copilot** can save real time on everyday work. This policy keeps that useful — protecting our clients, our information and our reputation — without burying anyone in red tape. It applies to everyone at [business name], including contractors.

2. The golden rules (the short version)

- **Never paste secrets.** No client personal information, passwords, financial details or anything confidential goes into a public AI tool.
- **Always check the output.** AI can be confidently wrong. You are responsible for anything you send, publish or act on.
- **You own the result.** AI assists; a person decides and signs off. “The AI said so” is never an excuse.
- **Use approved tools.** Stick to the tools listed below for work tasks. Ask before using a new one.
- **If in doubt, ask.** Not sure if something's OK? Check with [name / role] first.

3. Approved tools

These are the AI tools approved for work use, and what each is approved for. Update as your stack changes.

Tool	Approved for	Notes / account type
Claude (Anthropic)	[e.g. drafting, summarising long documents, review]	[e.g. Team plan — no training on our data]
ChatGPT (OpenAI)	[e.g. brainstorming, research starters, everyday drafts]	[e.g. Business/Enterprise account]
Microsoft 365 Copilot	[e.g. work inside Word, Excel, Outlook, Teams]	[e.g. licensed, data stays in our tenant]
[Other tool]	[what it's approved for]	[account / restrictions]

Anything not on this list is not approved for work data until [name / role] has signed it off.

4. What you can — and can't — put into AI

Generally OK (in approved tools):

- Public or non-sensitive information, and your own draft writing
- Realistic but made-up examples that stand in for real data
- Internal text with names, figures and identifying details removed

Never put into a public AI tool:

- Client or customer personal information (*names + details, health, financial, contact records*)
- Passwords, API keys, or anything from a password manager
- Confidential commercial information — contracts, pricing, unreleased plans
- Anything you wouldn't be comfortable seeing forwarded outside the business

5. Always check the output

- **Verify facts.** Check names, numbers, dates, quotes and any claim before relying on it.
- **Watch for made-up detail.** AI can invent sources, figures and references that look real.
- **Keep your voice.** Edit drafts so they sound like us, not like a robot.
- **Disclose where required.** Follow any client or industry rules about telling people AI was used.

6. Privacy & client data

We protect personal information in line with our obligations under the **Australian Privacy Principles** and any client agreements. If a task needs real client data, use an **approved private or enterprise tool** where our data isn't used to train the model — never a free public chatbot. When unsure, treat data as sensitive and ask **[name / role]**.

7. Who's accountable

The person who uses AI for a task owns the result — same as if they'd done it by hand. Managers make sure their team understands this policy. Breaches are handled under our normal conduct process. Questions, ideas and “is this OK?” checks go to **[name / role]**.

8. Acknowledgement

I have read and understood the Team AI Usage Policy and agree to follow it.

--

Name

--

Signature

--

Date

Starter template, not legal advice. This is a practical starting point provided free by Digital Greenhouse. Adapt it to your business and, for anything with legal or regulatory weight, get professional advice. We can tailor this with your team as part of an AI training day — digitalgreenhouse.com.au/services/ai-training