Rangefront Labs

Template · Free resource

AI Acceptable Use Policy Template

Your staff are already using AI tools, with or without a policy. This editable template gives you a sensible AI acceptable use policy in plain English: what's allowed, what data is off-limits, and who's accountable, w...

Updated May 2026

https://rangefrontlabs.com.au/resources/ai-acceptable-use-policy-template/

Built in Toowoomba. Working across Australia and internationally.

Here's the uncomfortable truth: your team is already using AI. Someone pasted a client email into ChatGPT to soften the tone. Someone ran the quarterly numbers through a free tool to "just summarise it". That happened whether or not you have a policy: the only question is whether it happened *within sensible limits* or completely in the dark.

The job of an AI acceptable use policy is to give people clear, reasonable rules so they can use AI confidently without putting your clients' data, your IP, or your obligations at risk. Think of it as permission with guardrails, not a ban. This template is a sensible starting point written for Australian organisations. Fill in the brackets, cut what doesn't apply, and you have a usable policy in an afternoon.

Read it in full below, or download the editable version and make it yours.

When you need one

You need a policy the moment **any** of these are true, which for most businesses is already the case:

- Staff have access to general AI tools on work devices or accounts.
- Your work involves personal information, client data, or confidential material.
- You're in a regulated or contracted sector with privacy or security obligations.
- You want the productivity of AI without quietly accepting unmanaged risk.

The template

The full policy follows. Replace anything in **[square brackets]** with your own details, and delete clauses that don't fit. It's deliberately short: a policy people will actually read beats a forty-page document they won't.

[Organisation]: Artificial Intelligence Acceptable Use Policy

Effective date: [date] · **Owner:** [role, e.g. Operations Manager] · **Review:** every [6/12] months

1. Purpose

This policy sets out how people at [Organisation] may use artificial intelligence (AI) tools in their work. It exists so we can benefit from AI while protecting our clients, our people, our information and our legal obligations.

2. Who this applies to

All employees, contractors, and volunteers who use AI tools for [Organisation] work, on any device or account.

3. Our principles

- **People stay accountable.** AI assists; it never carries the final responsibility. A person owns every output that leaves [Organisation].
- **Protect information first.** When in doubt about whether something is safe to share with a tool, don't. Ask [role] instead.
- **Be honest about AI's role** where it matters to clients, accuracy or fairness.

4. Approved tools

Use only AI tools on the approved list maintained by [role]:

- [Tool 1, approved for: e.g. general drafting on non-sensitive content]
- [Tool 2, approved for: e.g. coding assistance]

Using a tool that isn't on the list for anything beyond open, public information requires approval from [role]. Free consumer tools must not be used for sensitive or restricted information.

5. What you must not put into AI tools

Unless the tool is specifically approved for it in writing, never enter:

- Personal information about clients, staff or third parties (names, contact details, health, financial or identity information).
- Confidential or commercially sensitive material: contracts, pricing, unreleased plans, credentials or passwords.
- Anything covered by a confidentiality agreement or by [Organisation]'s obligations under the Privacy Act 1988 (Cth).

If you're unsure whether information falls into these categories, treat it as if it does.

6. Human review

A person must review AI output before it is used externally, relied on for a decision, or treated as fact. AI can be confidently wrong. You are responsible for checking accuracy, tone, bias and appropriateness before anything goes out under [Organisation]'s name.

7. Prohibited uses

Do not use AI tools to:

- Make final decisions about people (hiring, discipline, eligibility) without human judgement and oversight.
- Generate content that is misleading, discriminatory, defamatory or unlawful.
- Impersonate a real person or misrepresent AI-generated content as solely human where that would deceive.
- Circumvent security controls or [Organisation] policies.

8. Transparency

Where AI has materially shaped work that affects a client or a decision about a person, disclose its involvement honestly if asked, and follow any sector-specific disclosure rules that apply to us.

9. Security and accounts

Use [Organisation] accounts and approved access only. Don't connect AI tools to our systems, data or email without approval from [role]. Report any suspected data exposure through an AI tool to [role/contact] immediately.

10. Intellectual property

Treat AI output as a draft, not a finished asset. Check that generated material doesn't reproduce someone else's protected work, and remember that the ownership and licensing of AI output can be unclear. Don't rely on it for anything where ownership matters without checking.

11. Breaches

Breaching this policy may lead to loss of AI tool access and, for serious or repeated breaches, disciplinary action. Tell us early if something goes wrong: a reported mistake is far easier to contain than a hidden one.

12. Questions and review

Questions go to [role]. This policy is reviewed every [6/12] months, or sooner if tools, risks or laws change.

How to adapt it

1. **Set the owner and the approved-tools list first.** A policy with no named owner and no list of allowed tools is just a wish.
2. **Match clause 5 to your real data.** A health provider, a law firm and a marketing agency have very different "never enter this" lists. Be specific.
3. **Decide your disclosure stance** in clause 8 based on your sector and clients.
4. **Make it findable and brief it in person.** A policy that lives in a folder nobody opens changes no behaviour. Walk the team through it once.

Common mistakes

- **Banning everything.** A total ban doesn't stop AI use; it just pushes it onto personal accounts where you have no visibility at all. Permit and guide instead.
- **Writing it once and forgetting it.** The tools change monthly. A policy that isn't reviewed is out of date within a year.
- **No named owner.** "Everyone" owns it means no one does.

This template is a strong default, not legal advice. If your obligations are significant (health, finance, government, or anything heavily regulated), get it reviewed for your context. That, and rolling it out so people actually follow it, is exactly what we help with on a discovery call.

Need this adapted to your organisation, systems or data? Book a discovery call: https://rangefrontlabs.com.au/contact/