

How to use this template

- Replace everything in [brackets] with your own decision. Bracketed text is shaded so you can find it.
- Delete this box before you share the policy.

Free template from Joring. Guidance on each decision: joring.ai/resources/ai-acceptable-use-policy-template

AI Acceptable Use Policy

Company	[Company name]
Policy owner	[name, role]
Backup	[name, role]
Effective	[date]
Last reviewed	[date]

1. Purpose and scope

We want everyone at [Company] to use AI to do better work, faster, without putting customer, employee or company information at risk. This policy explains which AI tools you may use, what information you can put into them, and makes clear the expectation that you are responsible for anything you create with AI.

It applies to all employees [, contractors and temporary staff] who use AI for [Company] work, on any device or account.

“AI tools” means any product that creates text, images, code, audio or analysis from a prompt. That includes chat assistants such as ChatGPT, Claude, Gemini and Microsoft Copilot, AI features inside other software, browser extensions, meeting note-takers and AI agents.

2. Who to ask

[Policy owner] owns this policy. Send questions, tool requests and reports of mistakes to [email or chat channel]. If [policy owner] is away, contact [backup].

3. Approved AI tools

You may use these tools for work, signed in with your company account:

- [Tool and plan, for example ChatGPT Business]: up to [Confidential] information
- [Tool and plan]: up to [Internal] information

- AI features inside software we already approve, such as [writing help in Microsoft 365 or Google Workspace]: same rules as the software itself

Don't use personal AI accounts for [Company] work, even for tools on this list. Personal accounts can let the vendor use what you type to improve its AI, and they aren't covered by our contracts. [Decide whether to allow any exceptions.]

4. Asking for a new tool

If you want to use a tool that isn't on the list, ask [policy owner] at [link or email]. We will check:

- whether the vendor trains its AI on our data, and whether we can turn that off
- how long it keeps our data and who can see it
- whether we have a business agreement that protects our information
- whether it fits what our customer contracts allow

We aim to answer within [five working days]. Until a tool is approved, use it only with Public information.

5. Information rules

Before you put anything into an AI tool, check which level it belongs to:

- **Public:** already published, such as our website, press releases and public documents. Fine in any tool.
- **Internal:** everyday work that isn't meant for outsiders, such as process documents and general meeting notes. Approved tools only.
- **Confidential:** customer and employee information, contracts, pricing, financial results, source code and unreleased plans. Only in tools approved for confidential information in section 3. [Remove names and account numbers first where you can.]
- **Never:** passwords, API keys and other credentials; payment card and bank account numbers; Social Security and other government ID numbers; health information; and anything a contract says we can't share. Never put these into any AI tool.

If you're not sure, treat it as the higher level or ask [policy owner]. [If you already have a data classification policy, use its levels here instead.]

6. What you can use AI for

Allowed (in approved tools, within the information rules):

- drafting and editing emails, documents and posts
- summarizing documents and meeting notes you're allowed to see
- brainstorming, first-pass research and explaining unfamiliar topics

- writing, explaining and reviewing code
- [your team's common tasks]

Ask [policy owner] first:

- uploading whole files or datasets that contain Confidential information
- creating content that will be published or sent to many customers at once
- using AI in a new customer-facing process, such as a support chatbot
- connecting AI to company systems (see section 10)

Never:

- making or recommending decisions about hiring, firing, pay, promotion or discipline (see section 9)
- creating content that is deceptive, discriminatory, harassing or illegal
- copying a real person's voice or likeness without their permission
- getting around this policy, for example by switching to a personal account when a work tool says no

7. Check AI output before you use it

AI tools can sound confident and still be wrong. They can invent facts, numbers, quotes, sources and legal citations. You are responsible for anything you create with AI.

Before AI-assisted work leaves your hands, check:

- facts, numbers, names and dates against a trusted source
- every link, quote and citation, by opening it
- whether it copies someone else's work, such as text, images or code
- code, by reviewing and testing it like any other code
- anything customers will see, for accuracy and tone

[For legal, financial, medical or safety content, a second person must review it: [role].]

8. Being open about AI use

Be honest about how you used AI. If someone asks, don't present AI work as entirely your own. Tell [your manager] when AI did most of the work on [a client deliverable or anything published under our name]. Tell customers they're dealing with AI when [for example, they're chatting with an AI assistant, or their contract requires it].

9. Decisions about people

Don't use AI to make or recommend decisions about hiring, firing, promotion, pay or discipline [unless [policy owner] and [HR or legal] have approved the tool and the process in writing]. Some laws require notices or bias audits for these uses.

10. Connecting AI to company systems

Get written approval from [policy owner] [and IT] before you:

- connect an AI tool to email, calendars, shared drives, customer records or code repositories
- install AI browser extensions or plug-ins
- use an AI meeting note-taker or recorder (and tell everyone in the meeting)
- set up AI agents that can act for you, such as sending messages, changing records or making purchases

11. Reporting mistakes

If you put information into the wrong tool, or AI output caused a problem, tell [policy owner] at [contact] within [24 hours]. Stop using the tool, keep a copy of what you entered and what it produced, and don't delete anything until [policy owner] says so. The sooner we know, the sooner we can fix it. [No one will be disciplined for promptly reporting an honest mistake.]

12. Training and acknowledgment

Everyone completes [a short AI training] when they join and [every year]. You'll be asked to confirm that you've read this policy. We keep a record of both.

13. How we check this policy is working

[Company] may review which AI tools are used on company devices, networks and accounts, to make sure this policy works and to learn which tools people need. [Describe what you review and how often.]

14. Breaking the rules

Breaking this policy is handled under [our disciplinary policy]. Nothing in this policy limits your rights under the law, including your right to discuss pay and working conditions. [Ask your lawyer whether to include this line.]

15. Review

[Policy owner] reviews this policy [every quarter or at least once a year], and also when we adopt a major new AI tool, a customer contract changes what we can do, a new law applies, or something goes wrong.

Acknowledgment

I have read and understand the AI Acceptable Use Policy.

Name

Signature

Date
