

# Sample AI Use Policy for a Small Business

A template from Blue Peak Data Consulting. Version 1.0, October 2026.

A sample policy written by Blue Peak for a business of roughly 10 to 75 people whose staff already use tools such as ChatGPT, Microsoft 365 Copilot, Claude or Gemini. Replace every bracketed item, delete what does not apply, and have the result read by your attorney and your IT provider before you adopt it. It is a template, not legal advice. It draws on NIST guidance (the AI Risk Management Framework, NIST AI 100-1, and its Generative AI Profile, NIST AI 600-1) and on the FTC's position that claims about AI must be true and substantiated; sources are listed at the end.

## 1. Purpose and scope

---

[Company] uses AI tools to work faster and better. This policy sets the rules so that use stays safe for our customers, our staff and the business. It applies to every employee, contractor and temporary worker, on any device, whenever the work is [Company]'s work. It covers general AI assistants, AI features inside software we already own (for example Copilot in Microsoft 365 or AI features in our accounting or CRM system), and any AI tool a vendor uses on our behalf.

## 2. Definitions

---

- **AI tool.** Any software that generates text, images, code, summaries, predictions or recommendations from a model, standalone or inside another product.
- **Approved tool.** An AI tool listed in section 3, used through a [Company] business account.
- **Confidential data.** Anything we would not publish: customer lists, pricing and margins, contracts, financial statements, payroll, personnel records, security details, unreleased plans, and anything given to us in confidence.
- **Personal data.** Anything that identifies a person: names with contact details, Social Security or tax numbers, dates of birth, card and bank numbers, health information, government ID numbers, photographs.
- **Human review.** A named person reads AI output in full and takes responsibility for it before it is used.

## 3. Approved tools

---

Only the tools below may be used for [Company] work. Personal accounts, free tiers and browser extensions that read page content are not approved, because their terms usually allow the vendor to keep and train on what is typed in. The policy owner (section 11) maintains this table and adds a tool only after reading its data terms.

| Tool                                      | Account          | Approved for                                                     | Not approved for                                 |
|-------------------------------------------|------------------|------------------------------------------------------------------|--------------------------------------------------|
| [Microsoft 365 Copilot, business licence] | [Company] tenant | Drafting, summarising, meeting notes, data already in our tenant | Final numbers without a check against the source |

| Tool                                                         | Account                           | Approved for                                     | Not approved for                                       |
|--------------------------------------------------------------|-----------------------------------|--------------------------------------------------|--------------------------------------------------------|
| [ChatGPT Business or Claude Team]                            | [Company] workspace, training off | Drafting, research, explaining, first-draft code | Confidential or personal data outside sections 4 and 5 |
| [AI features inside our accounting, CRM or ticketing system] | Existing business licence         | The tasks the vendor built them for              | Exporting data to other AI tools                       |

## 4. Data that never goes into an AI tool

---

Regardless of the tool or account, the following are never typed, pasted, uploaded or dictated into an AI tool:

1. Social Security numbers, tax IDs, driver's licence and passport numbers.
2. Card numbers, bank account numbers, and login credentials of any kind.
3. Health information about any person, including our own staff.
4. Payroll, compensation and performance records about named people.
5. Customer data a contract, a non-disclosure agreement or a regulator restricts (ask the policy owner if unsure).
6. Anything marked confidential by a customer or partner, unless the approved tool runs inside our own tenant and the policy owner has confirmed the data stays there.

If a task needs this data, remove or replace it first ("Customer A", "[amount]") or do the task without AI.

## 5. Acceptable use

---

**Encouraged.** First drafts of emails, documents and posts. Summaries of documents we are allowed to read. Rewriting for tone or length. Explaining unfamiliar terms. Brainstorming. Turning notes into action lists. Drafting formulas, scripts and checklists a person will test.

**Allowed with human review (section 6).** Anything that goes to a customer, a vendor, a regulator or the public. Anything with a number, a date, a price or a legal term in it. Anything used to make a decision about a person.

**Not allowed.** Using AI to make a final decision about hiring, firing, pay, credit or eligibility. Generating content that imitates a real person's voice or likeness without written permission. Uploading another company's confidential material. Using AI output as the only source for a factual claim in marketing. Bypassing a tool's safety settings or the approved-tools list.

## 6. Human review

---

AI output is a draft until a person has reviewed it. For [Company] that means:

- The person who sends or publishes it reads every line and owns it. "The AI wrote it" is never an explanation.

- Every number, date, name, quotation and citation is checked against the source. AI tools invent plausible references and get arithmetic wrong.
- Anything with legal, financial, safety or HR consequences gets a second reader, named in advance ([role]).
- Automations that act on their own (send, pay, delete, change a record) need a written design approved by the policy owner, with a human approval step and a log of every action.

## 7. Disclosure

---

- We tell customers when AI is part of a product or service they pay for, in plain words, and we do not call something "AI powered" unless it is.
- Claims we make about AI in our marketing are specific and substantiated, in line with the FTC's guidance. We do not promise results we have not measured.
- AI-generated images, voices or video in our materials are labelled where a reasonable viewer might assume otherwise.
- When a customer asks whether something was produced with AI, we answer honestly.

## 8. Security and accounts

---

- Business accounts only, with multi-factor authentication on, provisioned and removed by [IT provider or role] like any other account.
- Vendor terms are read before a tool is approved: where data is stored, whether it is used for training, how long it is kept, whether it can be deleted.
- Extensions and plug-ins come only from the approved list; devices follow our existing password and update rules.

## 9. Incidents

---

An AI incident is any of these: data entered into a tool against section 4; AI output sent out with a material error; an automation acting outside its design; a suspected account compromise; a complaint about our use of AI.

Report it to [policy owner] the same business day and do not delete the conversation or the output; it is the record. The policy owner records what happened, what was involved, who was affected and what was done, and decides with [management or counsel] whether a customer, partner or regulator must be told. Good-faith reports are never a disciplinary matter in themselves.

## 10. Training

---

- Every new starter reads this policy and completes a short walkthrough of the approved tools in their first two weeks.
- All staff attend a refresher at least once a year, or when the approved-tools list changes substantially.
- A prompt playbook of tested, role-specific examples is kept at [location]; questions and good examples go to [channel], so what works is shared.

## 11. Ownership, exceptions and review

---

The policy owner is [name and role]. They maintain the approved-tools list, record exceptions, receive incident reports and keep this document current. Exceptions are requested and answered in writing and expire on a date. This policy is reviewed every six months, or sooner if the law, our tools or our business change.

| Version | Date   | Change         | Approved by |
|---------|--------|----------------|-------------|
| 1.0     | [date] | First adoption | [name]      |

## 12. Acknowledgement

---

I have read the [Company] AI Use Policy, I understand it, and I agree to follow it.

Name: \_\_\_\_\_ Signature: \_\_\_\_\_ Date: \_\_\_\_\_

## Sources this template draws on

---

1. National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, January 2023. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>
2. National Institute of Standards and Technology, *AI RMF: Generative Artificial Intelligence Profile*, NIST AI 600-1, July 2024. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>
3. Federal Trade Commission, Business Blog, "Keep your AI claims in check," February 27, 2023. No longer published on [ftc.gov](https://www.ftc.gov); archived copy: <http://web.archive.org/web/20250101082345/https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check>
4. Federal Trade Commission, press release, "FTC Announces Crackdown on Deceptive AI Claims and Schemes," September 25, 2024. <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>

*A sample of Blue Peak's work. General information, not legal advice, and not reviewed for your business, state or industry; have your attorney review any policy before you adopt it. Blue Peak Data Consulting LLC, Olathe, Kansas. [bluepeakdataconsulting.com](https://bluepeakdataconsulting.com), (913) 777-4770.*