

[COMPANY NAME] — AI Acceptable Use Policy

Effective date: [DATE] · Version: [1.0] · Policy owner: [NAME / ROLE] · Review cycle: [Quarterly / Biannual]

1. Purpose

This policy explains how workers at [Company Name] may use artificial intelligence (AI) tools in the course of their work. Its goals are to let people use AI productively while protecting [Company Name]'s data, customers, employees, and legal obligations.

2. Scope

This policy applies to [all employees, contractors, interns, and temporary workers] who use [Company Name] devices, accounts, systems, or data. It covers all AI tools — generative AI assistants, AI writing and coding tools, AI meeting note-takers, and AI features built into other software — whether accessed through a company account or a personal account, when used for work purposes.

[Choose one: This policy applies to AI use on personal devices during work hours / only to company-owned devices and company accounts.]

3. Definitions

- "AI tool" — any software that uses machine learning or generative AI to produce text, code, images, audio, video, analysis, or decisions (for example ChatGPT, Claude, Microsoft Copilot, Gemini, and AI features embedded in other apps).
- "Confidential information" — [define for your company; e.g. customer data, employee and HR data, financial data, source code, contracts, and anything not already public].
- "Approved tool" — an AI tool [Company Name] has reviewed and authorized for the uses described in Section 5.

4. Roles and responsibilities

- Employees are responsible for following this policy and for reviewing AI output before relying on it.
- Managers are responsible for communicating this policy to their teams and modeling compliant use.
- [Policy owner / role] owns this policy, maintains the approved-tool list, and handles questions and incidents.

5. Approved, limited, and prohibited tools (tool tier list)

[Company Name] classifies AI tools into three tiers. The current tier list is maintained at [link or location] and reviewed every [period]. Before using any AI tool that is not on the list, request approval from [role].

- **Tier 1 — Approved:** use freely for work tasks, subject to the data rules in Section 6. Examples: [ChatGPT Enterprise, Microsoft Copilot (enterprise), Claude Team].
- **Tier 2 — Limited:** permitted only for [specific tasks] and only with non-confidential data, or with prior approval from [role]. Examples: [free-tier consumer AI tools].
- **Tier 3 — Prohibited:** not approved for any work use. Examples: [tools with no data-processing agreement or unknown data handling].

6. Data handling rules

Do **not** enter the following into any AI tool unless that specific tool is approved for that data type:

- Customer or client personal data (names, contact details, account records)
- Employee or HR personal data
- Financial data, pricing, or unreleased financial results
- Proprietary source code, trade secrets, or product roadmaps
- Legal, contractual, or privileged information
- [Regulated data: health information / PHI, payment-card data, etc., if applicable]

Rule of thumb: if you would not post it publicly, do not put it into a non-approved AI tool. When in doubt, ask [role] before sharing.

7. Human oversight and accountability

The person who uses an AI tool is responsible for its output. All AI-generated work — emails, documents, code, and analysis — must be reviewed and verified by a qualified person before it is sent, published, or relied upon. AI must not make final decisions on [hiring, promotion, discipline, lending, or other high-stakes matters] without documented human review and sign-off.

8. Disclosure and transparency

Disclose AI use where required, for example: [AI-generated content shared externally with clients or the public; AI-assisted analysis in executive or board materials; AI used in any regulated process; AI-generated code deployed to production]. Follow any client or contractual disclosure requirements that apply to your work.

9. Acceptable uses

Encouraged uses, with non-confidential data and human review, include: drafting and editing, brainstorming, summarizing public material, writing and debugging code, research starting points, and learning.

10. Prohibited uses

Do not use AI tools to: enter prohibited data (Section 6); generate content that is unlawful, harassing, discriminatory, or infringing; present AI output as independently verified when it is not; attempt to bypass security or access controls; or make prohibited automated decisions (Section 7).

11. Incident reporting

If you accidentally share confidential data with an AI tool, act on harmful or incorrect AI output, or notice a possible policy violation, report it to [role / contact] promptly. Reporting is non-punitive; reporting early limits harm.

12. Enforcement

Violations may result in [graduated consequences: a coaching conversation, a formal warning, up to termination] depending on severity and intent, consistent with [Company Name]'s [disciplinary / HR] policies.

13. Review schedule

This policy is reviewed at least every [six months] and is updated when major AI tools change their data practices, when a new tool category becomes widely used, or when relevant regulations change. Policy owner: [name / role].

14. Employee acknowledgment

By signing below, I confirm that I have read and understood [Company Name]'s AI Acceptable Use Policy and agree to follow it.

Employee name: _____

Signature: _____

Date: _____

Not legal advice. This template is provided for general informational purposes only and does not constitute legal advice. AI regulations vary by jurisdiction and industry and change frequently. Have your policy reviewed by qualified legal counsel before you adopt or rely on it.