

AI Acceptable Use Policy

Sample for public use. Replace [Company] with your name.

Purpose

This policy says how [Company] may use artificial intelligence so people can get work done without putting client data, company data, or the business at risk. AI may help with work. It does not replace a person's judgment, and it does not remove anyone's responsibility for the result.

Scope

This policy applies to every employee, contractor, and temporary worker, and to every AI tool used for company or client work. That includes chat tools, writing assistants, image tools, meeting summarizers, browser extensions, and anything similar that is added later.

Principles

1. Sensitive information stays out of tools that are not approved.
2. A person is accountable for every output that is used.
3. Only approved tools are used for company work.
4. If you are not sure, you ask before you paste.

1. Acceptable use

People may use approved AI tools to:

- Draft, summarize, or edit content that is not confidential
- Brainstorm ideas, outlines, and first drafts
- Research public information
- Analyze data that has been approved and stripped of anything sensitive
- Speed up repetitive work, with a person still checking it

A person must review the output before it is used in client communication, an operational decision, or anything financial, legal, or safety-related.

2. Prohibited use

People may not:

- Put client data, personal information, health information, payment data, passwords, or security details into an AI tool unless that tool has been approved for that use
- Put pricing, contracts, unpublished work, or other company intellectual property into a public or personal AI tool

- Let AI make a decision on its own about a client, money, hiring, safety, or compliance
- Use AI to skip an approval, an audit step, or a security control
- Use a public AI tool to train a model on company or client information
- Use a personal AI account for company or client work

3. Data handling

Do not enter the following unless the tool is approved and the use is written down:

- Client records or personally identifiable information
- Health information
- Financial or payment information
- Passwords, keys, or how our systems are set up
- Internal process, pricing, or unpublished work

You may use public information, anonymized data, and content that has been explicitly approved for AI.

Meeting recordings and transcripts count as company data. Do not drop them into a tool that stores or trains outside [Company].

Treat every AI answer as unverified until a person checks it.

4. Tool approval

Only tools that IT (or the owner, if there is no IT person) has approved may be used for company work.

Approval should look at how the vendor handles data, whether it trains on what you type, how long it keeps it, who can see it, and whether that fits the company's legal and contract duties.

Free consumer tools and browser add-ons are not approved by default. A new tool needs a yes before anyone uses it for work. Approved tools should be reviewed again when the vendor changes how data is used.

5. Accountability

AI output is a draft. The employee who uses it owns the accuracy and the outcome. Mistakes, odd results, or a suspected leak get reported to a manager the same day.

6. Training

People complete a short AI briefing before they use approved tools. It covers what they may do, what they may not paste, and the fact that AI can be wrong or biased. The briefing is updated when the tools change.

7. Enforcement and review

Use that does not follow this policy can mean loss of access to AI tools and other discipline, up to termination, depending on what happened.

[Company] will review this policy at least once a year, when the law changes, or when a new kind of AI tool is brought in. Changes are given to everyone this policy covers.

Questions go to [IT contact or owner].