



FREE TEMPLATE · VERSION 1.0 · OCTOBER 2026

AI Use Policy Template for Small Businesses

A ready-to-adopt policy for using AI at work: one governed AI tool for the whole team, clear rules for what information can go in, and a human approval on anything that moves money.

- 1 Fill in one page
- 2 Have your attorney review it
- 3 Train your team
- 4 Roll it out

WorkflowLoom

AI enablement, workflow automation and AI agents for small and mid-sized businesses
Bartlesville, Oklahoma · workflowloom.com

A practical starting point, not legal advice. Have your attorney review before you adopt it.

Read me first

This template gives a small business a complete AI use policy in an afternoon. It is built on one idea: pick one governed AI tool for the whole team, be clear about what information can go into it, and keep a person in charge of anything that moves money.

How to use this template

- 1 **Fill in the Policy Details page (page 3).** Every company-specific detail the policy refers to, such as the Approved AI Tool, the AI Administrators and the deadlines, comes from that page. Type it once and the policy is complete.
- 2 **Pick one approved AI tool** and enter it on the Policy Details page. The policy works with any business-grade AI tool that gives you company-owned accounts and admin controls. The point is one governed tool, not which brand.
- 3 **Add to the "Always a person" list in Section 9, never subtract.** There is a field for it. If your business has other actions that move money or grant access (releasing orders, issuing credits, changing pricing in your systems), list them there.
- 4 **Need different examples or wording?** The examples in Section 5 are deliberately general. To swap in the documents your people actually handle, or to change any wording, use the editable Word version of this template.
- 5 **Have your attorney review it before you adopt it.** This template is a practical starting point, not legal advice. Employment law, privacy rules and your client contracts vary. Pay particular attention to Section 7 (ownership) and Section 14 (violations).
- 6 **Train before you hand out access.** A policy nobody has been walked through is shelfware. Training without a policy is how company information leaks. You need both.

Make it yours: logo and colors

- **Your logo (this PDF).** On the Policy Details page, click the dashed box and choose your logo file (PNG or JPG). This works in the free Adobe Acrobat Reader. Some other PDF apps, like Apple Preview or a web browser, can fill in the text fields but cannot add images.
- **Your colors and fonts (Word version).** The PDF keeps WorkflowLoom's design. To use your own brand colors, open the Word version: on the Home tab, right-click a heading style (Heading 1 or Heading 2), choose Modify, and pick your color. To recolor the table headers, click in a table, open Table Design, and change the Shading.
- **Your logo (Word version).** Double-click the header at the top of any page, right-click the placeholder logo, choose Change Picture, and select your file.
- **Lock it when you are done.** After filling in the fields, choose Print and select "Save as PDF" (or "Microsoft Print to PDF") to make a finished copy your team cannot accidentally edit.
- **Sharing it with your team.** The policy starts on page 3. Share or print from page 3 onward, and leave this page and the cover out.



Click the box to add your logo (free Adobe Acrobat Reader).

Policy Details

Fill in this page first. Throughout the policy, "the Company," "the Approved AI Tool," "the AI Administrators" and every deadline mean what is written here.

COMPANY NAME (THE COMPANY)

APPROVED AI TOOL

COMPANY EMAIL DOMAIN

AI ADMINISTRATOR 1 (NAME, ROLE)

AI ADMINISTRATOR 2 (NAME, ROLE)

AI ADMINISTRATOR 3 (OPTIONAL)

APPROVED AI LIST KEPT BY (NAME, ROLE)

REQUIRED TRAINING BEFORE ACCESS

PERSONAL-ACCOUNT CLEANUP DEADLINE

COMPANY SYSTEMS WHERE INFORMATION MAY BE KEPT

POLICY OWNER (NAME, ROLE)

VERSION

EFFECTIVE DATE

NEXT REVIEW (AT LEAST EVERY 6 MONTHS)

PRICING FOR LIVE BIDS AND QUOTES IS TREATED AS (SECTION 5)

YELLOW: company account only

RED: never without written approval

Tip: name at least two AI Administrators, so approvals and incident reports never wait on one person.

AI Use Policy

This policy applies to the Company named on the Policy Details page. Capitalized terms such as the Company, the Approved AI Tool and the AI Administrators mean what is written there.

1. Why this policy exists

AI tools can save real time on email, reports, proposals, research and everyday paperwork. They also make it easy to send company information to outside companies without meaning to. Once information goes into an outside AI service, the Company loses control of it: who sees it, how long it is kept, and whether it is used to train someone else's product.

The Company's information, and the know-how behind how we work, belongs to the Company. This policy keeps it that way while giving our people good AI tools to do their jobs.

2. Who this policy covers

- Every Company employee: full-time, part-time and seasonal, in the office or in the field.
- Owners, officers and managers.
- Contractors, consultants and temporary staff who handle Company information.
- Any device: company computer, personal computer, phone or tablet. If it involves Company work or Company information, this policy applies, on or off the clock.

"AI tools" means chat assistants, AI search, AI features inside other apps and websites, browser extensions, meeting recorders, and automations or agents that use AI.

3. The core rule

Company AI only. The only AI tool approved for Company work is **the Approved AI Tool named on the Policy Details page, through an account assigned by the Company and signed in with your company email address.** Every other AI tool, app, account or feature is off-limits for Company work unless an AI Administrator has approved it in writing.

This includes free tools, trial accounts, and accounts signed up with a personal email. A personal account of any kind, including a personal account on the same AI service the company uses, is not a Company account.

4. Not allowed for Company work

The following may **not** be used for anything related to Company work or Company information unless an AI Administrator approves it in writing. This list is examples, not a complete list. If a tool uses AI and the Company did not assign it to you, it is not allowed. The Approved AI Tool, used through your company account, is the one exception to this table.

Type	Examples (not a complete list, as of October 2026)
AI chat assistants	ChatGPT, Claude, Google Gemini, Microsoft Copilot, Perplexity, Meta AI, Grok, DeepSeek, Mistral Le Chat, Poe, and any personal account on any of them
AI search and browsers	Perplexity, Google AI Mode, ChatGPT search, AI browsers, "summarize this page" browser features
AI inside other apps and social media	Meta AI in Facebook, Instagram, WhatsApp and Messenger; Snapchat My AI; AI features in Notion, Canva, Grammarly, Adobe Acrobat, Zoom, Google Docs and Gmail
Meeting recorders and notetakers	Otter.ai, Fireflies, Read.ai, Fathom, tl;dv, Zoom AI Companion, Teams or Google Meet AI notes
Writing, image, voice and video tools	Jasper, Copy.ai, QuillBot, Midjourney, DALL-E, Sora, ElevenLabs, HeyGen
Coding tools	GitHub Copilot, Cursor, Windsurf, Replit, Lovable, Bolt
Phone apps and extensions	AI apps on personal phones, AI keyboards, AI browser extensions

The same rule applies to AI features inside software the Company already uses (accounting, CRM, project management, scheduling, PDF and document software). Leave those features off until an AI Administrator approves them.

5. What information can go in

Before you paste or upload anything, ask one question: what is this, and which account am I in?

Level	What it means	Examples	Rule
GREEN	Public or general information	Published standards and regulations, manufacturer and product information, public web content about the Company, general how-to questions	OK in the company account.
YELLOW	Internal company information	Internal emails, meeting notes, schedules, draft proposals and letters, reports, procedures, project and job files	Company account only. Never in a personal or unapproved tool.
RED	Highly sensitive	Social Security numbers, medical information, pay and personnel records, bank and card numbers, passwords and access codes, anything a client contract says cannot be shared	Never , even in the company account, without written approval from an AI Administrator.

When in doubt, treat information as one level higher, or ask.

Company know-how is company information. The processes, procedures, checklists, pricing methods, templates and systems the Company has developed are company intellectual property, just as much as financial or personal data. Treat them as YELLOW at minimum. Pricing for live bids and quotes is treated at the level chosen on the Policy Details page.

6. Client and third-party documents

Documents from clients, partners and vendors may be covered by confidentiality terms or copyright.

- 1 **Check the contract before you upload.** Look for confidentiality, non-disclosure or data-handling language.
- 2 **Upload only what you need.** One section is better than the whole document.
- 3 **Do not upload a document if the terms say not to.**
- 4 **When you are not sure, ask** an AI Administrator first. Asking costs a few minutes. A breach of a client's terms can cost the relationship.

7. Company information and ownership

All Company information stays inside Company systems: the company systems listed on the Policy Details page, the company account in the Approved AI Tool, and other systems the company has approved. It never goes into a personal or unapproved AI tool.

Everything created with company AI tools belongs to the Company. Prompts, chats, projects, files and results made in the company account are company property and stay with the company when someone leaves.

8. Using your company AI account

Do:

- Use only the account assigned to you, signed in with your company email address, with multi-factor authentication turned on.
- Keep company work in the company account, in shared company workspaces where it makes sense.
- Read and check everything the AI produces before you use it. You are responsible for it.
- Have a qualified person check anything involving pricing, quantities, schedules, safety, technical or engineering judgment, or contract and legal language.
- Verify facts, figures and sources yourself. AI can sound certain and still be wrong, and it can cite pages that do not say what it claims.
- Ask an AI Administrator when you are unsure.

Don't:

- Share your login or let anyone else use your account.
- Use your company account for personal business, side jobs or other employers.
- Enter RED information without written approval.
- Let AI make safety, legal or engineering decisions. It can help draft; qualified people decide.
- Let AI send email, submit forms, make purchases, or sign or accept terms on the Company's behalf without approval.
- Connect the AI tool to other company systems (email, file storage, accounting or other software) yourself. Connections are set up only by an AI Administrator.
- Record or transcribe meetings with AI without approval and without telling everyone in the meeting.
- Publish AI-written content (website, social media, proposals, bids) without a person reviewing and approving it.

Away from your desk: don't photograph documents, screens or work you're doing into AI apps on your phone. If AI could help with something in the field, ask your supervisor or an AI Administrator.

9. AI automations, agents and approvals

This section covers automations and AI agents: anything that reads, writes, sends or changes things on the Company's behalf without a person doing each step. Only an AI Administrator can set one up or change it.

Every automation gets an approval level, based on two questions: how easy is the action to undo, and how much damage could it do if it is wrong?

Level	What the automation does	Rule
Runs on its own	Drafts, summaries, internal notes, and writes to internal records that are easy to undo	May run without approval, but every run is logged.
Approved until proven	Sends anything outside the company: email, messages, documents, quotes	A person approves each send. An AI Administrator may later move it to spot-checks or limits, in writing, once there is a track record.
Always a person	Moves money, changes where money goes, or touches access	A person approves every single time. This level never relaxes.

"Always a person" includes, at minimum:

- Payments, refunds, credits and payroll changes.
- Any new vendor or payee, and any change to a vendor's or payee's bank details, remit-to address or payment instructions.
- Passwords, logins, user accounts and permissions.
- The first message to any new recipient sent in the Company's name.

ALSO "ALWAYS A PERSON" AT THE COMPANY (ADD YOURS, NEVER REMOVE ANY ABOVE)

Verify bank-detail changes outside the request. A request to change where money is sent is the most common business email fraud there is, and it often arrives looking exactly like a real vendor. Before anyone approves a bank or remit-to change, call the vendor on a phone number already on file, never one from the email or invoice that asked for the change. Never approve a change by replying in the same email thread that asked for it: if that mailbox has been taken over, your reply goes straight to the fraudster.

The approval screen must show what is actually happening: the exact amount, the recipient, and what changed from before. A bare "Approve?" button is not an approval. If you cannot see what you are approving, do not approve it, and tell an AI Administrator. If nobody answers an approval request, nothing happens: an unanswered approval never counts as a yes.

A clean track record does not remove an "Always a person" approval. Months of smooth runs prove the normal case works. Approvals exist for the unusual case: a bad or tampered input, a vendor that changes its invoice format, an AI model update. Those are exactly the cases a long quiet stretch never tests. If an automation that was moved to spot-checks sends something wrong, or its AI model, the software it connects to, or the format of what it reads changes, it goes back to a person approving every send until it earns a new track record.

10. AI Administrators, accounts and exceptions

AI Administrators: the people named on the Policy Details page.

- **Accounts** are assigned by role. To request one, ask an AI Administrator. Everyone completes the required training named on the Policy Details page before getting access.
- **Exceptions:** if you need a different AI tool or feature, or need to use RED information, send a written request (email is fine) to an AI Administrator saying what the tool is, what you would use it for, and what information would be involved. Do not use it until you have written approval.
- **Approved list:** approved tools and exceptions are kept on the company's approved AI list, maintained by the person named on the Policy Details page.

11. Moving off personal AI accounts

Anyone who has used a personal or unapproved AI account for Company work must, by the cleanup deadline on the Policy Details page:

- 1 Stop using it for Company work immediately.
- 2 Tell an AI Administrator which accounts were used.
- 3 Work with an AI Administrator to export anything useful and bring it into the company account.
- 4 Delete all Company information from the personal account (chats, files, projects, custom assistants, saved memories and shared links), and confirm in writing that it is done.

Nobody is in trouble for past use that they disclose and clean up through this process.

Personal use of your own AI account for non-company matters is your business. Keep it fully separate from company work.

12. Company accounts are not private

Company AI accounts are company property. The Company may review activity and content in company AI accounts, to the extent the account plan allows, and may remove access at any time. Do not put personal matters in your company account.

13. Reporting mistakes

If you put Company information into the wrong tool, or you're not sure whether you did, **tell an AI Administrator right away**: what it was, which tool, and roughly when. Don't try to fix it quietly first. Fast reporting lets us limit the damage. An honest mistake reported promptly is treated very differently from one that is hidden.

14. Violations

Following this policy is a condition of using Company information and systems. The following are serious violations:

- Using a personal or unapproved AI tool or account for Company work.
- Putting Company information into any AI tool outside the company account.
- Going around the approval process, or using a tool before written approval.
- Turning off, skipping or working around an automation's approval step.
- Sharing company AI logins, or using a company account for non-Company work.
- Hiding or failing to report a known misuse.

Violations may result in disciplinary action, up to and including termination of employment. The Company may also take other steps to protect its information, including legal action where appropriate.

15. Questions and review

- Questions go to any AI Administrator.
- **Policy owner:** named on the Policy Details page. This policy is reviewed at least every six months, and whenever the company's AI tools change.
- **Effective date:** as shown on the Policy Details page. It becomes part of the employee handbook once adopted.

Acknowledgement

I have read and understand the Company's AI Use Policy. I agree to follow it. I understand that violations may result in disciplinary action, up to and including termination.

NAME (PRINT)	SIGNATURE	DATE

Keep one signed acknowledgement per person on file with the AI Administrators.

A policy is step one. Rolling it out (choosing the tool, setting up accounts, training each role, an

I've read this. Remove the WorkflowLoom note above. (This line does not print.)