

[COMPANY NAME]

Artificial Intelligence (AI) Use Policy

Template for small businesses and professional practices

Policy owner	[Name, title]
Approved by	[Owner / managing partner]
Effective date	[Date]
Next review	[Date, at least every 6 months]
Applies to	All employees, contractors, interns and anyone using company systems or client data

How to use this template

- Replace everything in [BRACKETS]. Delete any section that doesn't apply, and delete this how-to section once you're done.
- Fill in the Approved Tools list (Section 4) before you share the policy. A policy without a tool list gets ignored.
- If you're in a regulated field (law, healthcare, accounting and tax, financial advice, insurance, real estate), read the matching addendum in Appendix B and have your compliance advisor or counsel review the final version.
- Have every staff member sign the acknowledgment in Appendix C, and keep the signed copies.

This template is general information, not legal advice. Laws and vendor terms change; check the sources in Appendix D before you adopt it.

1. Purpose

[COMPANY NAME] encourages the use of AI tools that help us serve clients faster and better. This policy sets the rules so that we use AI safely: protecting client and company information, keeping a qualified person responsible for every piece of work, and meeting our legal and professional obligations.

2. Scope

This policy covers any software that generates or analyzes text, images, audio, video or code using AI, including chat assistants (for example ChatGPT, Claude, Gemini, Copilot), AI features built into software we already use (email, CRM, practice management, accounting, design and phone systems), meeting recorders and note-takers, browser extensions and AI agents that can take actions on our behalf. It applies on company devices and on personal devices used for work.

3. Core rules (the short version)

1. Use only tools on the Approved Tools list, with your company account.

2. Never put Restricted information into an AI tool unless that tool is approved for it (Section 5).
3. A qualified person reviews and is accountable for anything AI helps produce before it goes to a client, patient, customer, court, regulator or the public.
4. Check facts, numbers, citations and quotes against the original source. AI can state false things confidently.
5. Don't use AI to make final decisions about people (hiring, firing, credit, pricing for an individual, eligibility) without human review and approval from [ROLE].
6. Tell [POLICY OWNER] right away if something goes wrong, such as confidential data entered into the wrong tool or an AI error that reached a client.

4. Approved tools

Only the tools below may be used for work. To request a new tool, email [POLICY OWNER] with the tool name, what you want to use it for and a link to its data/privacy terms. [POLICY OWNER] will check it using the vendor checklist in Appendix A.

Tool / plan	Approved uses	Highest data level allowed	Settings required	Owner
[e.g., ChatGPT Business]	[Drafting, summarizing, research]	[Internal / Confidential]	[Company workspace only; data not used for training]	[Name]
[e.g., meeting note-taker]	[Internal meetings; client calls only with consent]	[Confidential]	[Recording notice on; retention 90 days]	[Name]
[e.g., AI in practice-management software]	[Scheduling, reminders]	[Restricted, with signed agreement]	[BAA / DPA on file]	[Name]

Free or personal versions of AI tools are not approved for company or client information unless they appear in this list.

5. What information can go into AI tools

Data level	Examples	Rule
Public	Published website copy, public laws and regulations, press releases	Any approved tool
Internal	Internal procedures, templates, non-sensitive drafts, anonymized examples	Any approved tool, signed in with a company account
Confidential	Client names and matters, contracts, pricing, financials, unpublished plans, employee information	Only tools approved for Confidential data in Section 4. Remove what isn't needed.
Restricted	Social Security and tax ID numbers, bank and card numbers, passwords and API keys, health information	Never, unless the tool is approved for Restricted data, the required agreement (for example a HIPAA

	(PHI), tax return information, privileged legal material, biometric data, anything a contract or law says we must protect	business associate agreement or client consent) is in place, and [POLICY OWNER] has signed off
--	---	--

When in doubt, treat information as the higher level, strip identifying details, or ask first.

6. Human review and accuracy

- The person who sends or files the work owns it, whether or not AI helped.
- Verify every fact, figure, quote and citation against the original source before use. For legal, tax, medical or financial content, a licensed or qualified person must review it.
- Don't paste AI output into client deliverables without reading all of it.
- Keep a note of significant AI use on client work (which tool, what for) in the file or matter record.

7. Transparency and disclosure

- Don't present AI-generated content as a human's personal statement when it isn't (for example, reviews, testimonials or signed letters).
- Never use AI to create fake reviews or testimonials, or to impersonate a real person.
- Tell clients when AI will be used in a way that affects their matter or fees, or when they'd reasonably expect to know. [Optional: add our standard client disclosure wording here.]
- If an AI phone, chat or texting agent talks to customers on our behalf, follow the disclosure, consent and recording rules for our state and industry. [List them here.]
- Label AI-generated or materially altered images and video where a platform, regulator or common sense requires it.

8. Intellectual property and copyright

- Don't upload content you don't have the right to use (for example, a competitor's materials or licensed content whose license forbids it).
- Purely AI-generated material may not be protected by copyright. If we need to own a deliverable (logos, key marketing assets, client work product), make sure a person contributes meaningful creative work and keep the drafts.
- Check AI images for trademarks, logos and recognizable people before publishing.

9. Fairness and decisions about people

AI must not be the sole basis for decisions about hiring, firing, promotion, pay, credit, housing, insurance or access to services. If we use AI anywhere in these processes, [ROLE] must approve it in advance, a person must review each outcome, and we will check our obligations under anti-discrimination law and any state or local rules on automated decision tools.

10. Security

- Use company accounts with multi-factor authentication. Don't share logins.
- Turn off model training on our data where the tool allows it, and set the shortest practical retention.
- Don't install AI browser extensions, plug-ins or agents that can read email, files or screens without approval.
- Don't give AI agents permission to send messages, make payments or change records without a person approving each action, unless [POLICY OWNER] has approved a specific, limited workflow.
- Report suspected data exposure immediately to [POLICY OWNER / IT CONTACT] at [EMAIL / PHONE].

11. Recording meetings and calls

- Get consent before recording or transcribing calls, following the strictest rule of any state the participants are in. Some states require every party's consent.
- Don't let a note-taker join client or patient calls unless the tool is approved for that data level.
- Delete recordings and transcripts according to our retention schedule: [X days].

12. Training

Everyone covered by this policy completes AI training when they join and [annually / every six months]: the core rules, our approved tools, data levels, and how to check AI output. [POLICY OWNER] keeps a record of completion.

13. Incidents and violations

Report mistakes quickly. We would much rather hear about a problem early. Incidents include confidential data entered into an unapproved tool, AI errors that reached a client, and suspicious AI-generated messages (for example, voice-cloned calls asking for payments or passwords). Violations of this policy may lead to discipline, up to and including termination, consistent with our other policies.

14. Review

[POLICY OWNER] reviews this policy and the Approved Tools list at least every six months and whenever we adopt a major new tool or the law changes.

Appendix A. Vendor checklist for approving an AI tool

Question	Answer / link
Does the vendor use our inputs or outputs to train its models? Can we turn that off?	
How long does it keep our data? Can we set retention or delete on request?	
Where is data stored and processed? Which subprocessors (including AI model providers) see it?	
Security: SOC 2 Type II or ISO 27001 report available? MFA and single sign-on?	
Will it sign the agreement our field requires (HIPAA business associate agreement, data processing agreement, confidentiality terms)?	
Who owns the outputs? Any IP indemnity?	
Admin controls: can we see who uses it, manage accounts and remove access when someone leaves?	
Price, contract length, renewal and cancellation terms	
Decision, approved data level and date	

Appendix B. Industry addenda (keep the ones that apply)

Law firms

Follow ABA Formal Opinion 512 (July 2024) and your state bar's guidance: understand the tool well enough to use it competently, protect client confidentiality (informed client consent may be needed before entering client information into some tools), verify all output (including every citation), supervise staff use, and bill fairly for AI-assisted work. Check your courts' standing orders on AI disclosure in filings.

Healthcare (dental, medical, therapy)

Protected health information may go only into tools covered by a signed HIPAA business associate agreement that covers the AI features you use. Apply the minimum-necessary standard. Confirm reminder and outreach texting follows the FCC's TCPA rules and your state's rules.

Accounting and tax

Tax return information is protected under Internal Revenue Code section 7216 and its regulations; don't disclose it to a third-party tool without meeting those rules (including written client consent where required). Follow your information security plan (WISP) under the FTC Safeguards Rule, and the AICPA's guidance for AI use.

Financial advisors and insurance

Keep AI-generated client communications and meeting notes under your books-and-records and supervision rules (SEC, FINRA or state insurance regulators as applicable). Don't let AI make suitability or coverage recommendations without a licensed review.

Real estate

Listing descriptions and ads must comply with the Fair Housing Act: describe the property, never the kind of buyer or renter. Follow your MLS rules on virtually staged or AI-edited photos, including labeling and keeping the original.

Marketing and sales

Follow the FTC's rule banning fake reviews and testimonials (16 CFR Part 465, effective October 2024) and its Endorsement Guides. Get consent and follow TCPA rules before AI-generated calls or texts.

Appendix C. Employee acknowledgment

I have read the [COMPANY NAME] AI Use Policy, I understand it, and I agree to follow it. I understand that I'm responsible for work I produce with AI tools and that violations may lead to discipline.

Name	
Role	
Signature	
Date	

Appendix D. Sources

- NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), January 2023: <https://www.nist.gov/itl/ai-risk-management-framework>
- American Bar Association, Formal Opinion 512: Generative Artificial Intelligence Tools, July 29, 2024: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf
- U.S. HHS, Business Associates (HIPAA): <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>
- IRS, Section 7216 information center: <https://www.irs.gov/tax-professionals/section-7216-information-center>
- FTC, Final rule banning fake reviews and testimonials (August 2024): <https://www.ftc.gov/news-events/news/press-releases/2024/08/federal-trade-commission-announces-final-rule-banning-fake-reviews-testimonials>
- FTC Safeguards Rule: <https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know>
- U.S. Copyright Office, Copyright and Artificial Intelligence, Part 2: Copyrightability (January 2025): <https://www.copyright.gov/ai/>
- HUD, Fair Housing Act overview: https://www.hud.gov/program_offices/fair_housing_equal_opp/fair_housing_act_overview

More playbooks for your field: <https://aiforthework.com/>