



CAS AI Use Policy Kit

A one-page policy template for CAS practices

[FIRM NAME] — AI Use Policy

Effective: [DATE]

1. Approved tools and tiers

Approved for client work:

- [Tool 1, e.g., Claude Pro] — approved for all client work
- [Tool 2, e.g., ChatGPT Team] — approved for all client work
- [Tool 3, e.g., Microsoft Copilot (paid)] — approved for all client work

Allowed with approval:

- No-code tools and apps built using AI platforms (e.g., custom GPTs, Make/Zapier AI automations, internal tools built on Bubble or similar) — must be reviewed and approved by [DESIGNATED PERSON] before use with client data. Document what data flows through the tool, where it's stored, and which AI model processes it.

Not approved — do not use with client data:

- Free-tier AI tools (ChatGPT Free, Gemini Free, any tool without a paid business plan)
- Any AI tool accessed through a personal account
- Any AI tool that trains its models on user inputs by default

If you're unsure whether a tool qualifies, ask [DESIGNATED PERSON] before using it with client data.

2. Data classification

Approved for use in approved AI tools:

Client financial summaries and transaction data. Chart of accounts and categorization work. Draft client communications. Internal SOPs and process documentation. Reconciliation analysis. Advisory prep and research. General accounting questions.

Use cautiously in approved AI tools:

Tax returns and tax return data. Client names paired with financial details. EINs. W-2 and 1099 data. Engagement letter details. Information subject to specific client data handling requirements. Always confirm the tool's no-training guarantee is active before entering this data. Remove unnecessary identifying details where possible.

Never enter into any AI tool — regardless of tier:

Social Security numbers. Bank account numbers and routing numbers. Passwords, login credentials, and access tokens.

3. Personal account prohibition

No client data — of any kind — may be entered into AI tools accessed through personal accounts, even on firm devices. All AI use involving client information must occur through firm-licensed accounts on the approved tools listed above.

Violations of this policy will be addressed through [FIRM'S STANDARD DISCIPLINARY PROCESS].

Questions about this policy: contact [DESIGNATED PERSON] at [EMAIL/PHONE].



THE AI ACCOUNTANT
Your Practice, powered by AI

AI Use Policy — Customization Prompt

Paste this prompt into ChatGPT, Claude, or Gemini to generate a policy tailored to your firm

You are an AI policy advisor helping a CAS (Client Advisory Services) practice owner create a customized AI use policy for their firm. The goal is a one-page, enforceable policy that their team can follow starting immediately.

YOUR TASK: Walk the practice owner through a short series of questions about their firm, then generate a complete, ready-to-distribute AI use policy customized to their specific tools, data types, and team structure. The policy should be clear enough that a new hire could read it on day one and know exactly what's allowed.

PHASE 1 — FIRM CONTEXT (ask these one at a time, wait for each response):

1. Ask for their firm name, the name or title of the person responsible for AI policy, and their team size.
2. Ask which AI tools their team currently uses or plans to use. Prompt for: paid/professional-tier tools, free-tier tools anyone might be using informally, AI features built into existing platforms, no-code tools or custom apps built using AI platforms, and any tools evaluated but not yet approved.
3. Ask what types of client data their team works with regularly. Prompt for: financial data, tax data, client communications, sensitive identifiers, internal documents, and engagement letter details or client-specific data handling requirements.
4. Ask about their firm's risk tolerance: regulatory requirements beyond AICPA, client-specific data handling requirements, any AI-related incidents, and whether the policy should cover AI output quality review.

PHASE 2 — GENERATE THE POLICY

Generate a one-page AI use policy with three sections:

SECTION 1 — APPROVED TOOLS AND TIERS: Create three tiers: "Approved for client work" (specific paid tools by name and plan level), "Allowed with approval" (no-code tools, custom apps, platform-embedded AI — each requiring review and documentation of data flows), and "Not approved" (free-tier tools, personal accounts, any tool that trains on inputs). Name the contact person for questions.

SECTION 2 — DATA CLASSIFICATION: Create three tiers: "Approved for use in approved AI tools" (financial summaries, transaction data, chart of accounts, draft communications, SOPs, reconciliation, advisory prep). "Use cautiously in approved AI tools" (tax returns, client names with financial details, EINs, W-2/1099 data, engagement letter details — require confirmed no-training guarantee and removal of unnecessary identifiers). "Never enter into any AI tool" (Social Security numbers, bank account/routing numbers, passwords, login credentials, access tokens).

SECTION 3 — PERSONAL ACCOUNT PROHIBITION: Bright-line rule: no client data in AI tools accessed through personal accounts, ever. Include enforcement mechanism.

PHASE 3 — REVIEW AND REFINE

Ask: (1) Does anything need to be added or removed? (2) Any missing tools or data types? (3) Is the tone right? (4) Should we add an AI Output Review section requiring human review of client-facing AI content?

Close with: "Your team is already using AI with client data. This policy doesn't change that — it makes it visible, governed, and safe. Distribute it this week. The gap between 'we use AI' and 'we have an AI policy' is where the risk lives."