AI Acceptable Use Policy Template

For small and mid-sized businesses | Free, editable template from JR Secure Design Inc.

How to Use This Template

This template is a ready-to-edit starting point for an AI Acceptable Use Policy. It sets clear, practical rules for how your employees and contractors may use generative AI tools such as ChatGPT and Microsoft Copilot at work.

1. Replace every bracketed field, such as [Company Name], [Policy Owner], [Effective Date], [Approved Tools], and [Contact Email], with your own details.
2. Delete anything that doesn't apply to your business, and add rules specific to your industry or clients.
3. Fill in the Approved AI Tools table with the tools and account types you actually allow.
4. Have leadership and legal counsel review the final version, then share it with staff and collect signed acknowledgements.

This template is not legal advice. Have your legal counsel review it before adopting it.

[Company Name] AI Acceptable Use Policy

Policy owner	[Policy Owner, Name and Title]	**Effective date**	[Effective Date]
Approved by	[Approver Name and Title]	**Version**	[Version Number]
Questions	[Contact Email]	**Next review**	[Next Review Date]

1. Purpose and Scope

Purpose. [Company Name] supports the responsible use of artificial intelligence (AI) to help people work better. This policy explains which AI tools may be used, how to use them safely, and what is not allowed, so we protect our clients, employees, data, and reputation.

Scope. This policy applies to all employees, contractors, interns, and temporary staff ("users"); to all AI tools used for company work on any device, including AI features built into other software (email, office, CRM, design, or meeting tools); and to all company, client, and employee information. It works alongside our [Information Security Policy], [Data Classification Policy], [Privacy Policy], and [Code of Conduct]. If policies conflict, follow the stricter rule and ask [Policy Owner].

2. Definitions

- **AI tool:** Any software or service that uses AI to generate, summarize, analyze, translate, or transform content, including chatbots, writing and coding assistants, image/audio/video generators, meeting note-takers, and AI features inside other applications.
- **Prompt / output:** A prompt is anything you give an AI tool (text, files, images). An output is anything it produces.
- **Approved tool:** An AI tool listed in Section 3.1 or approved in writing under Section 8.
- **Company-managed account:** An account created and controlled by [Company Name] through a business or enterprise subscription and company sign-in, not a personal or free account.
- **Shadow AI:** Any AI tool, account, extension, plugin, or integration used for company work without approval.
- **Connector, plugin, or agent:** An add-on that lets an AI tool access other systems (email, files, websites) or take actions on your behalf.

3. Approved and Prohibited Tools

3.1 Approved AI Tools

Only the tools below (or tools later approved under Section 8) may be used for company work, with company-managed accounts, for the uses listed. The current list is kept at [Location of Approved Tools List].

Tool	Account required	Approved uses	Highest data level allowed	Tool owner
[Approved Tool 1, e.g., ChatGPT Business or Enterprise]	[Company workspace, company sign-in]	[e.g., drafting, summarizing]	[e.g., Internal]	[Name/Role]
[Approved Tool 2, e.g., Microsoft 365 Copilot]	[Company Microsoft 365 account]	[e.g., email, documents, meetings]	[e.g., Confidential, per labels]	[Name/Role]
[Approved Tool 3]	[Account Type]	[Approved Uses]	[Data Level]	[Name/Role]

3.2 Prohibited Tools and Uses

- **Personal or free AI accounts for work.** Never use a personal, free, or consumer account of any AI tool for company or client work, even if the same product is approved under a company account.
- **Shadow AI.** Do not use any AI tool, app, or service that is not approved.
- **Unapproved browser extensions, plugins, and add-ons.** Do not install AI extensions, plugins, note-takers, or add-ons for browsers, email, documents, or meetings unless approved. Many can read everything on your screen, in your inbox, or in a meeting.
- **Unapproved connectors and agents.** Do not connect AI tools to company email, files, calendars, code repositories, or business systems, or let an AI agent act on your behalf, without approval.
- **Recording without consent.** Do not use AI recorders or transcription tools without approval and without notifying participants as our policy and applicable law require.
- **Harmful, deceptive, or unlawful use.** No discriminatory, harassing, defamatory, or explicit content; no impersonating real people (including voice or video deepfakes); no fake reviews or testimonials; no bypassing security controls or generating malicious code.
- **[Other prohibited uses specific to your business].**

4. Data That Must NEVER Go Into AI Tools

Unless a specific tool has been approved in writing for that type of data, **never** enter, paste, upload, or connect the following to any AI tool:

Category	Examples
Client confidential information	Client files, contracts, pricing, strategy, anything covered by an NDA or client agreement
Personally identifiable information (PII)	Social Security, driver's license, or passport numbers; dates of birth; personal contact details of customers or employees
Protected health information (PHI)	Medical records, diagnoses, treatment, insurance or benefits details tied to a person
Payment and financial data	Card numbers, bank account and routing numbers, tax records
Credentials and secrets	Passwords, API keys, access tokens, private or encryption keys, MFA codes, connection strings
Source code and trade secrets	Proprietary code, product designs, formulas, unreleased financials, deal plans (unless the tool and use are approved)
HR and security information	Performance, pay, or disciplinary records; network diagrams, vulnerability reports, incident details
[Other Restricted Data]	[Examples specific to your business or industry]

When in doubt, leave it out. Remove names and identifying details first, share only the minimum needed, or ask [Policy Owner].

5. Using ChatGPT and Microsoft Copilot

ChatGPT and Microsoft Copilot may be used for company work **only** through company-managed business accounts that IT has set up and configured.

5.1 ChatGPT

- Use only [Company Name]'s **ChatGPT [Business / Enterprise]** workspace, signed in with your company account. Never use a personal or free ChatGPT account for work.
- OpenAI states that it does not train its models on business customers' data by default. IT confirms this and other workspace settings at setup and at each review. Do not change data-sharing settings yourself.
- Admins manage workspace controls, such as who can join, sign-in method, which GPTs, apps, and connectors are allowed, data retention, and sharing outside the company.
- Section 4 still applies inside the company workspace.

5.2 Microsoft 365 Copilot

- Use only **Microsoft 365 Copilot** (or Copilot Chat) signed in with your company Microsoft 365 account, never consumer Copilot or a personal Microsoft account.
- Microsoft 365 Copilot respects existing Microsoft 365 permissions: it can find and summarize any file, email, chat, or site you already have access to. **If content is overshared, Copilot can surface it.**
- Before rollout, IT will review and fix oversharing in SharePoint, OneDrive, and Teams (for example, sites or links open to everyone), apply sensitivity labels to confidential content, and confirm data protection and retention settings. [Owner: IT Lead] [Target Date]
- Apply the correct sensitivity label to documents you create, and never remove or downgrade a label to get around restrictions. If Copilot shows you something you should not see, stop and report it (Section 10).

5.3 AI Features in Other Software

AI features built into other applications count as AI tools. Do not turn them on for company data until they are approved under Section 8.

6. Human Review of AI Outputs

You are responsible for any work you produce with AI. AI can be confidently wrong.

- **Accuracy:** Verify facts, figures, names, quotes, links, and citations before using or sharing an output. Do not rely on AI for final legal, medical, financial, or safety advice.
- **Bias:** Review outputs for biased, offensive, or exclusionary content, especially anything about people or groups.
- **Intellectual property:** Do not use outputs that may copy someone else's protected work, trademarks, or likeness. Check with [Legal Contact] before using AI content in products, marketing, or client deliverables where ownership matters.
- **Code:** Review, test, and scan AI-generated code through our normal development process before use.
- **No automated decisions about people:** AI must never be the sole basis for decisions that significantly affect people, such as hiring, firing, pay, promotion, discipline, or access to services. A qualified person must review and decide.

7. Disclosure and Labeling

- **Clients and customers:** Tell clients when AI materially produced content or analysis in a deliverable, or when a contract requires it. Follow any client restrictions on AI use. [Disclosure wording, e.g., "Portions of this document were drafted with AI assistance and reviewed by our team."]
- **Public content:** Label AI-generated images, audio, and video that could be mistaken for real people or events. [Where labels go]
- **Chatbots:** If customers interact with an AI assistant on our behalf, make clear it is AI and offer a way to reach a person.

8. AI Tool Request and Approval Process

To request a new AI tool, feature, extension, connector, or a new use of an approved tool, submit a request to [Request Channel or Contact Email]. Do not use the tool while the request is pending.

Request form fields: requester name and department; tool name, vendor, and website; business purpose; expected users and licenses; data types involved (see Section 4); systems it will connect to; plan type, sign-in method, and cost; vendor terms on training, retention, and data location; and the business owner after approval.

1. **Security and privacy review** by [IT/Security Lead]: vendor security, data handling and training settings, admin and access controls, logging, and integrations.
2. **Legal/contract review** by [Legal Contact] when client data, personal data, or new contract terms are involved.
3. **Decision** by [Approver, e.g., Policy Owner or AI Governance Committee] within [Number] business days ([Number] days for higher-risk requests).
4. **Record:** Approved tools are added to Section 3.1 with any conditions. Denials include a reason and, where possible, an approved alternative.

9. Training

All users complete AI acceptable use training [within Number days of hire] and [annually] after that, with extra training before using higher-risk tools such as connectors, agents, or coding assistants. Training covers this policy, safe data handling, spotting inaccurate or harmful outputs, and incident reporting. [HR or Policy Owner] tracks completion.

10. Incident Reporting

Report AI incidents to [Contact Email or Reporting Channel] **immediately, and no later than [Number] hours** after you discover them. For a possible data breach, also notify [Security Contact]. We will not retaliate against anyone for reporting in good faith.

Report it if:

- Sensitive data (Section 4) was pasted, uploaded, or connected to any AI tool.
- A personal, free, or unapproved AI tool, extension, or plugin was used with company or client data.
- An AI tool showed you information you should not have access to, or an agent or connector took an unexpected action.
- A harmful, biased, or seriously wrong output was shared, published, or used in a decision.
- You suspect AI-enabled phishing, impersonation, or a deepfake targeting [Company Name].

Include what happened, when, which tool and account, and what data was involved. Do not delete evidence; follow instructions from [Security Contact].

11. Enforcement

Violations may lead to loss of AI tool access and disciplinary action, up to and including termination of employment or contract, under our [Disciplinary Policy]. [Company Name] may monitor company systems and company-managed AI accounts consistent with applicable law and our [Monitoring/Privacy Policy], and may block unapproved tools. Exceptions require written approval from [Policy Owner], with a reason and an end date.

12. Policy Owner and Review Cycle

[Policy Owner, Name and Title] ([Contact Email]) owns this policy. It and the approved tools list are reviewed **[every 6/12 months]**, and sooner after a major new AI tool, a vendor terms or settings change, a significant incident, or new legal or contract requirements. As an optional reference, [Company Name] may use the NIST AI Risk Management Framework (AI RMF) to identify and manage AI risks.

Version	Date	Summary of changes	Approved by
[1.0]	[Effective Date]	Initial policy	[Approver]

13. Employee Acknowledgement

I have received, read, and understand the [Company Name] AI Acceptable Use Policy. I agree to use only approved AI tools with company-managed accounts, never enter prohibited data into AI tools, review AI outputs before using them, and report AI incidents promptly. I understand that violations may result in disciplinary action.

Employee name (print)		**Signature**	
Job title / department		**Date**	

Return the signed acknowledgement to [HR Contact or Contact Email] by [Due Date].

Template provided by JR Secure Design Inc. | jrsecuredesign.com | Need help rolling out AI governance? Book a strategy call: https://calendly.com/jdecrescenzojr/30min

This template is not legal advice. Have your legal counsel review it before adopting it.