

DOCUMENT 1 OF 4 · AI WORKPLACE POLICY KIT

AI Workplace Use Policy

Template for Small Businesses

This template provides a complete starting point for establishing your company's official policy governing the use of artificial intelligence tools by employees. Customize the bracketed fields with your company's specific information, approved tools, and requirements.

WHAT'S IN THIS KIT

- ✓ Scope and applicability statement
- ✓ Approved and prohibited AI tool categories
- ✓ Data handling and confidentiality rules
- ✓ Employee responsibilities and accountability
- ✓ Incident reporting procedures
- ✓ Policy acknowledgment signature block

NOT LEGAL ADVICE: This document is designed for small business compliance as a starting point. Have a qualified attorney review any legal or compliance document before relying on it for legal or regulatory purposes.

AI WORKPLACE USE POLICY

[COMPANY NAME]

Effective Date: [DATE] · Version: 1.0 · Owner: [HR/OPERATIONS/IT]

1. Purpose

[COMPANY NAME] recognizes that artificial intelligence (AI) tools offer significant productivity benefits and competitive advantages. This policy establishes guidelines for the responsible, safe, and compliant use of AI tools by all employees, contractors, and other personnel acting on behalf of [COMPANY NAME]. The goal is to enable productive AI use while protecting our clients, our data, and our business.

2. Scope

This policy applies to all employees, contractors, temporary workers, and any other individuals who use AI tools in connection with their work for [COMPANY NAME], regardless of whether the tool is company-provided or personally owned.

3. Definitions

AI Tool: Any software application, platform, or service that uses artificial intelligence, machine learning, or large language models to generate, analyze, summarize, translate, or otherwise process content. This includes but is not limited to chatbots, writing assistants, image generators, meeting transcription tools, and code assistants.

Confidential Information: Any information that is not publicly available, including but not limited to client data, financial information, employee records, proprietary business processes, trade secrets, and any information subject to a non-disclosure agreement.

Approved AI Tool: An AI tool that has been reviewed and approved by [DESIGNATED APPROVER] for use in connection with company work. See Appendix A for the current approved tools list.

4. Approved AI Tools

Employees may only use AI tools that appear on the company's Approved AI Tools List (Appendix A / Document 2 of this kit). Using an unapproved AI tool for work purposes is a policy violation. To request approval for a new AI tool, submit a request to [DESIGNATED APPROVER] using the AI Tool Request Form [LINK/LOCATION].

5. Prohibited Uses

The following uses of AI tools are strictly prohibited:

- Inputting client names, contact information, financial data, health information, or any other personally identifiable information (PII) into any AI tool not specifically approved for that purpose.
- Inputting confidential business information, trade secrets, proprietary processes, or unreleased product information into any AI tool.

- Using AI tools to generate content that will be presented to clients or published externally without human review and approval.
- Using AI tools to make final decisions about hiring, firing, performance evaluation, credit, or other consequential matters affecting individuals.
- Using AI tools to circumvent security controls, access unauthorized systems, or engage in any activity that violates applicable law.
- Using personal AI tool accounts (free tiers) for work purposes when a company-approved account with data protection controls is available.

6. Data Handling Requirements

Before using any AI tool for work purposes, employees must:

- Verify the tool appears on the Approved AI Tools List.
- Confirm that data retention and training opt-out settings are configured as required by this policy.
- Ensure that any client data shared with an AI tool is permitted under the applicable client agreement.
- Never share data that is subject to regulatory protection (HIPAA, FERPA, PCI-DSS, etc.) with an AI tool unless the tool has been specifically approved for that data category.

7. Output Review Requirements

AI-generated content must be reviewed by a qualified human before being used in any of the following contexts: client deliverables, legal or compliance documents, financial calculations, medical or health-related advice, public communications, or any content that will be presented as the work of [COMPANY NAME]. Employees are responsible for the accuracy of any AI-assisted work they submit or publish.

8. Employee Responsibilities

- Read, understand, and comply with this policy.
- Complete the AI Safety Training course within [30/60/90] days of hire and annually thereafter.
- Report any suspected AI-related security incidents, data exposures, or policy violations to [DESIGNATED CONTACT] within 24 hours of discovery.
- Keep AI tool credentials secure and not share accounts with other employees.
- Stay informed about updates to the Approved AI Tools List.

9. Incident Reporting

If you believe confidential information has been inadvertently shared with an AI tool, or if you discover a security vulnerability in an approved AI tool, report it immediately to [DESIGNATED CONTACT] at [EMAIL/PHONE]. Do not attempt to investigate or remediate the incident yourself. See Document 3 of this kit for the full AI Incident

Response Checklist.

10. Policy Violations

Violations of this policy may result in disciplinary action up to and including termination of employment, and may also result in legal liability. Suspected violations should be reported to [HR/MANAGER/DESIGNATED CONTACT].

11. Policy Review

This policy will be reviewed and updated at least annually, or more frequently as AI tools and regulations evolve. The current version is always available at [LOCATION]. Employees will be notified of material changes.

NOT LEGAL ADVICE: This template is a starting point designed for small business compliance. Have a qualified attorney review this policy before implementation, particularly if your business handles regulated data (health, financial, legal) or operates in a jurisdiction with specific AI regulations. — AIWatchdog · aiwatchdog.com