AI / POLICY / DATA PROTECTION

AI Acceptable Use Policy

A practical policy for small businesses that want employees to use AI tools without leaking sensitive company, customer, or regulated data.

Purpose

This policy explains how employees may use artificial intelligence tools for business work. The goal is to allow useful AI-assisted work while protecting company data, customer information, regulated data, credentials, and private business records.

Scope

This policy applies to all employees, contractors, temporary workers, and vendors who use AI tools while performing work for the company.

Covered tools include public AI chatbots, AI search tools, coding assistants, meeting transcription tools, document summarizers, browser-based AI tools, built-in office suite AI features, and locally hosted AI systems.

Approved uses

Employees may use approved AI tools for:

- Drafting non-sensitive emails, outlines, summaries, and planning notes
- Brainstorming ideas that do not include private company information
- Rewriting public-facing content
- Creating first drafts of procedures, checklists, or training material
- Summarizing public documents or public web content
- Explaining general technical concepts
- Writing or reviewing code that does not include secrets, proprietary logic, or customer data

Prohibited uses

Employees must not enter the following into public AI tools unless the company has formally approved that tool for the specific data type:

- Customer names paired with addresses, phone numbers, account numbers, records, or service history
- Protected health information, medical records, insurance information, or patient details
- Payment card data, bank account details, tax IDs, or payroll records
- Passwords, API keys, private keys, tokens, certificates, session cookies, or recovery codes
- Internal network diagrams, firewall rules, VPN details, vulnerability reports, or security incidents
- Confidential contracts, bids, pricing models, financial statements, or acquisition discussions
- Source code that contains secrets, proprietary algorithms, customer-specific logic, or non-public product details

- Employee disciplinary records, HR records, background checks, or compensation details
- Legal correspondence or privileged material

Data handling rule

If the data would be risky to email to an unknown third party, do not paste it into a public AI tool.

When in doubt, remove names, account numbers, identifiers, credentials, and business-sensitive details before using AI. If the work cannot be done safely without those details, ask a manager or the IT/security contact before proceeding.

Approved tools

The company will maintain a list of approved AI tools and approved use cases. Employees may not assume that a tool is approved because it is popular, free, built into a browser, or available on a personal phone.

Approved tools should be reviewed for:

- Data retention and training settings
- Account ownership and administrative controls
- Audit or logging options
- Enterprise privacy terms
- Multi-factor authentication support
- Ability to disable data training where needed

Human review

AI output must be reviewed by a person before it is used for business decisions, customer communication, policy, security work, legal work, medical work, financial work, or public publication.

Employees are responsible for verifying facts, tone, calculations, citations, and recommendations. AI output may be incomplete, outdated, biased, or incorrect.

Customer and regulated data

Customer data and regulated data require extra care. Employees may not use public AI tools to process protected health information, payment data, private customer records, or regulated records unless the company has approved the tool and the use case in writing.

For healthcare environments, do not enter patient information into public AI systems unless the company has confirmed that the tool, contract, and workflow support the required privacy and security obligations.

AI-generated content

Employees must disclose AI assistance when required by company process, customer contract, professional standards, or law. AI-generated content should not be presented as expert analysis unless a qualified person has reviewed and accepted responsibility for it.

Account security

Employees using approved AI tools must:

- Use company accounts when available

- Use multi-factor authentication
- Avoid signing into business AI tools with personal email accounts
- Avoid installing AI browser extensions without approval
- Report suspicious AI tool behavior, unexpected data exposure, or accidental sensitive data entry

Incident reporting

If sensitive information is entered into an AI tool by mistake, employees must report it promptly. A fast report gives the company the best chance to assess exposure, rotate credentials, notify affected parties if needed, and prevent recurrence.

Reports should include:

- The tool used
- The approximate time
- The type of data entered
- Whether the data included credentials, customer records, regulated data, or security details
- Any output the tool returned

Enforcement

Misuse of AI tools may result in access restrictions, retraining, disciplinary action, contract termination, or other measures based on risk and company policy.

Review schedule

This policy should be reviewed at least annually and whenever the company adopts a new AI tool, changes data handling practices, or enters a regulated business relationship.

Implementation checklist

- Publish the approved AI tool list
- Disable training on company data where the vendor supports it
- Require company-owned accounts for business use
- Add AI use expectations to onboarding
- Train employees on what not to paste into AI
- Create a simple incident reporting path
- Review browser extensions that add AI features
- Revisit the policy every 6 to 12 months

Disclaimer

This starter policy is general information, not legal advice. Adapt it to your business, contracts, regulatory obligations, and state law.