AI Acceptable Use Policy

Simple rules for employees and contractors using AI for work at [Company name]. You are responsible for the work you produce, even when AI helps.

Effective date: [Date] | Policy owner: [Name / contact]

1 Use approved tools

Use only the AI tools and company accounts on the approved list. Follow any limits shown there. Ask before trying a new tool or connecting AI to company systems.

2 Protect company and personal information

Never enter passwords or access keys into AI. Do not share confidential files, source code, customer records or personal information unless the tool and that use of the data are specifically approved. Share only what is needed.

3 Check before you use or share

AI can be wrong. Check facts, sources, calculations and possible bias. Make sure you have permission to use the content. Review and test AI-generated code. A person must check work before it reaches a customer, is published or supports an important decision.

4 Get approval for important actions

Do not let AI send messages, change records, make purchases or take other actions without approval for that use. Keep a person responsible for decisions affecting people, health, money or legal rights. Follow company rules on telling others when AI was used.

5 Use AI responsibly

Do not use AI to deceive, impersonate, harass, discriminate, break the law or bypass company rules. Follow the same standards you would when doing the work yourself. Complete any training your company requires.

6 Report problems quickly

Stop the affected activity and report suspected data leaks, harmful output, unexpected actions or account misuse through the company reporting channel. Do not put sensitive information in a public ticket. If you are unsure, ask before continuing.

Company Setup Checklist

For the policy owner: complete this checklist before sharing the employee policy. Keep the setup details available to everyone.

1 Name the owner and dates

Company: [Company name]. Policy owner and contact: [Name / contact]. Approved by: [Name / role]. Effective date: [Date]. Next review: [Date]. Review at least every six months and after important changes.

2 Publish the approved tools list

Approved tools and company accounts: [List or link]. For each tool, state what work and data are allowed, what is prohibited and who owns it. Have IT/security check access, storage, deletion and whether company data is used to train the tool. Involve privacy or legal specialists where needed.

3 Make help and reporting easy to find

New tool or use approval: [Contact / request channel]. Questions about this policy: [Contact]. Report a problem: [Security contact / channel]. Reporting target: [Company deadline]. Related company rules: [Links]. Make this information available with the policy.

4 Approve and share the policy

Complete every placeholder and confirm the rules fit your company. Get the appropriate security, privacy and legal review. Share the employee policy and setup details; explain the rules and record acknowledgement using your normal process. Record exceptions with an owner and expiry date. Handle misuse through existing company procedures.