AI Acceptable Use Policy Template

How to use this: Adapt this template to your organization's tools, data classifications, and approval process, then have leadership approve it before any AI tool is used for work. Review it at least every [6/12] months, and whenever a new AI tool is introduced.

---

1. Purpose

This policy sets out how employees of [Company Name] may and may not use artificial intelligence (AI) tools for work. It exists so staff can benefit from AI tools while protecting company data, client data, and the organization's legal and regulatory obligations.

2. Scope

This policy applies to:

- All employees, contractors, and temporary staff of [Company Name].
- Any AI tool used for work, whether provided by the company or accessed personally, including chatbots, writing assistants, coding assistants, image and video generators, and meeting transcription tools.
- AI features built into software the company already licenses (for example, AI assistants inside [productivity suite / CRM / email platform]).

3. Definitions

Term	Meaning
AI tool	Any software that generates text, images, code, audio, video, summaries, or recommendations using a machine learning model.
Approved AI tool	An AI tool listed in Section 4 that the organization has reviewed and approved for work use.
Confidential information	Non-public information belonging to the company, its clients, or its partners, including pricing, contracts, strategy, and internal discussions.
Regulated data	Data subject to specific legal or contractual handling rules, such as export-controlled data, health information, or financial records.
Personal data	Information relating to an identifiable individual, including names, contact details, and employee records.

4. Approved AI Tools

Only tools on this list may be used for work. A tool is added to the list only after review by [IT / Security / Governance Committee].

Tool	Approved uses	Data allowed	Owner
[Tool name]	[e.g., drafting, summarizing, brainstorming]	[e.g., public and internal non-confidential data only]	[Role / Name]
[Tool name]	[Approved uses]	[Data allowed]	[Role / Name]
[Tool name]	[Approved uses]	[Data allowed]	[Role / Name]

Do not use an AI tool for work if it is not on this list. To request a new tool, submit [request process / form] to [Owner].

5. Data That May Be Entered into AI Tools

You may enter the following into an approved AI tool, provided the tool's data handling has been reviewed:

- Publicly available information (for example, published reports, public web pages).
- Internal non-confidential material, such as draft wording for a public announcement, general process descriptions, and anonymized examples.
- Your own original drafts and notes, where they contain no confidential, personal, or regulated data.

Before entering anything, ask: "Would I be comfortable if this text appeared in a public place?" If the answer is no, do not enter it.

6. Data That Must Never Be Entered into AI Tools

Never enter the following into any AI tool, including approved tools, unless a specific written exception has been granted by [Governance Committee / Data Protection Officer]:

- Personal data of employees, clients, or any other individual (names, addresses, phone numbers, email addresses, identification numbers, salary or health details).
- Client confidential information, including client names in connection with their non-public business, contracts, pricing, or correspondence.

- Regulated data, including export-controlled technical data, data covered by [CUI / ITAR / EAR / HIPAA / other regulation], and data under a non-disclosure agreement.
- Company confidential information, including financial results, strategic plans, unreleased products, and security credentials.
- Usernames, passwords, API keys, tokens, or any other credentials.
- Source code, system configurations, or internal network details, unless the tool is an approved coding assistant and the code contains no credentials or confidential data.
- Any document marked [Confidential / Internal Only / Restricted].

If you are unsure whether data may be entered, treat it as prohibited and ask [Owner].

7. Using AI-Generated Output

AI output is a draft, not a finished product. The following rules apply:

- **Human review is required.** Read and check every AI-generated output before you use it, send it, or act on it. You are responsible for what you send, even if an AI tool produced it.
- **Verify facts, figures, and citations.** AI tools can produce plausible but incorrect information, including invented references. Check every fact, number, date, and quotation against a reliable source before relying on it.
- **Do not use AI output to make high-stakes decisions on its own.** Decisions about hiring, performance, pricing, contracts, safety, or compliance must be made by a person using AI output only as an input.
- **Do not present AI output as your own unaided work** where original authorship matters, such as in compliance statements, certifications, or client deliverables that imply human authorship. Disclose AI assistance where [Company Name] or the recipient requires it.
- **Correct errors.** If you find an AI output is wrong, do not forward it. Correct it, or do not use it.

8. Prohibited Uses

Do not use AI tools to:

- Generate misleading, deceptive, or false content, including fake reviews, fabricated evidence, or impersonation of any person.
- Produce content that discriminates against, harasses, or defames any person or group.

- Circumvent security controls, generate malicious code, or attempt to access systems without authorization.
- Create or distribute content that infringes intellectual property, including reproducing copyrighted text or images beyond fair use.
- Make automated decisions about individuals (for example, screening job applicants) without a documented human review step.
- Share AI-generated content externally as if it were an official company position without the approvals that would apply to the same content written by a person.

9. Training and Accountability

- All staff must complete [AI acceptable use training] before using AI tools for work, and refresher training [annually / when the policy changes].
- Managers are responsible for ensuring their teams understand this policy and for raising questions to [Owner].
- Questions about this policy should go to [Owner / email address].

10. Violations and Reporting

- If you believe data has been entered into an AI tool in breach of this policy, report it to [Owner] as soon as possible. Prompt reporting is treated as responsible behavior; concealing an incident is not.
- Breaches may result in [consequences per company disciplinary process, e.g., retraining, loss of AI tool access, disciplinary action].
- Suspected security incidents involving AI tools should also be reported through [incident reporting process].

11. Policy Review

Item	Detail
Policy owner	[Role / Name]
Approved by	[Role / Name]
Effective date	[Date]
Next review date	[Date]

Item	Detail
Version	[Number]

Employee Acknowledgment

I have read and understood this AI Acceptable Use Policy. I understand I am responsible for checking AI output before using it and for never entering prohibited data into AI tools.

Name	[Employee name]
Signature	
Date	[Date]