ComplyJet

AI Acceptable Use Policy

A free, editable employee policy for AI tools: nine clauses with sample wording, an AI tool register, a "can I paste this" card, disclosure wording, enforcement steps and an acknowledgement form.

HOW TO USE THIS TEMPLATE
Replace every [bracketed value] with a fact about your own company, delete anything that does not apply, fill the AI Tool Register in Appendix A from the tools your team actually uses, and publish only after counsel or your HR lead has read it. Delete this box and the next one before you publish.

BEFORE YOU PUBLISH
This template is a starting point, not legal advice. Contract and legal disclosure duties depend on your customers, your industry and where you operate. Tool tiers name categories, never endorse a vendor.

[Company Name] AI Acceptable Use Policy

Owner	[Role]
Effective date	[Date]
Next review	[Date, at least annually]
Applies to	Employees, contractors, interns and anyone using [Company Name] accounts, data or devices

Tool tiers and data rules at a glance

Tier	What qualifies	Who decides	Default
Tier 1: Company-managed	Company-owned account or workspace, signed data terms, training on company data switched off, admin can add and remove users	Tool owner with security sign-off	Approved for named use cases
Tier 2: Approved with limits	Reviewed for specific tasks and data classes only	Tool owner	Approved up to the class on the register
Tier 3: Not approved yet	Anything not on the register, including every personal account of any product	None yet	Not allowed for company data
Tier 4: Banned	Reviewed and refused, reason recorded	Policy owner	Never

Data allowed by tier

Data class	Tier 1	Tier 2	Tier 3	Tier 4
Public	Allowed	Allowed	Allowed with approval	Never
Internal	Allowed	Allowed	Never	Never
Confidential	Allowed	Never	Never	Never
Restricted	Allowed with approval	Never	Never	Never

Policy clauses

Clause 1: Purpose, Scope and Definitions

1.1 This policy sets the rules for using AI tools in work for [Company Name]. It applies to all employees, contractors, interns and any other person using [Company Name] accounts, data or devices.

1.2 "AI tool" means any software that generates, summarizes, translates, transcribes or analyzes content using machine learning, including chat assistants, coding assistants, meeting recorders, browser extensions, agents, and AI features built into other software.

1.3 "Company data" means any information held by [Company Name] that is not public. Data is classified as Public, Internal, Confidential or Restricted under the [Data Classification Policy].

Clause 2: Approved Tools and the Tool Register

2.1 AI tools are placed in one of four tiers: Tier 1 (company-managed), Tier 2 (approved with limits), Tier 3 (not approved) and Tier 4 (banned).

2.2 The approved tools and the data classes each may receive are listed in the AI Tool Register, owned by [Role]. The register is available at [location].

2.3 Any AI tool not on the register is Tier 3 until reviewed. A personal account on any tool, including a tool that is Tier 1 when used through the company workspace, is Tier 3.

2.4 Requests to add a tool are made using the form in Appendix A and answered within [5] working days.

Clause 3: Permitted Uses

3.1 You are encouraged to use approved AI tools for drafting and editing text, summarizing public or Internal material, brainstorming, explaining code, translating Internal text, and similar productivity tasks.

3.2 Use the tier of the tool and the class of the data to decide what is allowed, as set out in Section 4 and Appendix B.

3.3 If you are unsure whether a use is allowed, ask [Role or channel] before you proceed.

Clause 4: Data Rules and Prohibited Inputs

4.1 Public data may be used with Tier 1 and Tier 2 tools. Internal data may be used with Tier 1 and Tier 2 tools. Confidential data may be used with Tier 1 tools only. Restricted data may be used with a Tier 1 tool only after written approval from [Role] for that use case.

4.2 You must never enter the following into any AI tool unless a Tier 1 approval says otherwise: passwords, API keys and other secrets; regulated personal or health data; payment card data; customer data without a contract that allows it; other people's confidential information.

4.3 Where possible, remove names and identifiers or use sample data.

4.4 Use only your company account or workspace. Do not use a personal account for any company data above Public.

Clause 5: Human Review and Accountability

5.1 You are responsible for any work you produce with AI assistance. Check facts, sources, figures and code before you use or share them.

5.2 AI output must be reviewed by a person before it is sent to a customer, published, merged into production, or relied on for a business decision.

5.3 AI tools must not be the sole basis for decisions about hiring, firing, promotion, discipline, credit, or any person's legal rights.

Clause 6: Disclosure of AI Use

6.1 You must tell your manager when AI materially shaped a work product, if asked.

6.2 You must disclose AI use in a deliverable to a customer or other outside party when a contract, law or [Company Name] policy requires it, using the wording in Appendix B or the wording the contract specifies.

6.3 You must not present AI output as the work of a named individual who did not review it.

Clause 7: Intellectual Property and Customer Obligations

7.1 Do not enter material owned by a third party, or covered by a customer contract, into an AI tool unless the contract or licence permits it.

7.2 Do not assume AI output is free of third-party rights. Treat it as a draft that needs review before it is used in a product, a publication or a customer deliverable.

7.3 Before using AI on work delivered to a customer, check the customer agreement for restrictions on AI use or subprocessors. If in doubt, ask [Role].

Clause 8: Reporting Incidents and Concerns

8.1 If you enter data into an AI tool that this policy does not allow, report it to [channel or Role] within [24] hours of noticing.

8.2 Prompt, honest reporting will be treated as a mitigating factor. Concealing a mistake will not.

8.3 [Company Name] will not retaliate against anyone who reports a concern about AI use in good faith.

Clause 9: Exceptions, Violations and Review

9.1 Exceptions are requested in writing, approved by [Role], recorded in the AI Tool Register, and expire after [12] months unless renewed.

9.2 Violations of this policy are handled under the enforcement steps in Appendix C and [Company Name]'s existing disciplinary process.

9.3 This policy is reviewed at least [annually], and after any significant new AI tool, customer requirement or change in law. Every person covered by it acknowledges it at onboarding and at each review.

Appendix A: AI Tool Register and approval request

One row per tool. Anything not listed is Tier 3 until reviewed. Requests are answered within [5] working days.

Tool	Tier	Data classes allowed	Owner	Reviewed	Notes
[Tool name]	[1-4]	[Public / Internal / Confidential / Restricted]	[Role]	[Date]	[Notes or reason]

Approval request

Request field	Answer
What data will go in?	
Which plan and terms apply?	
Who will own the tool?	
What is it for?	
When will it be reviewed again?	

Appendix B: "Can I paste this?" card and disclosure wording

> **FIVE QUESTIONS, TEN SECONDS. STOP AT THE FIRST NO.**
>
> 1. Is this tool on the register?
> 2. Am I logged in with my company account, not a personal one?
> 3. Does the data class in the register allow this tool to take it?
> 4. Would I be comfortable if the customer saw exactly what I am pasting?
> 5. If I am about to share the output outside the company, has a person checked it?

Disclosure rules

Output type	Disclosure rule
Internal draft or note	None needed
Customer deliverable	Disclose if contract or law requires it; human sign-off always
Code in the product	Human review before merge; note in the pull request if your engineering policy asks
Marketing or published content	Human edit before publishing; label where law or platform rules require
Hiring or HR decisions	Never AI-only; tell the manager how AI was used
Regulated outputs	Follow the regulator's rule; ask [Role] first

Sample label where one is needed: This content was created with the assistance of AI tools and reviewed by [Company Name].

Appendix C: Enforcement steps and acknowledgement

Step	Typical trigger	Who acts	What is recorded
1. Coaching conversation	First minor breach	Manager	Short note in the policy owner's log
2. Written notice and retraining	A repeat, or Internal data in a Tier 3 tool	Manager and HR	Notice, training, new acknowledgement
3. Tool access removed	Confidential data in a banned tool, or ignoring step 2	Policy owner	Access change, reason, review date
4. Formal discipline	Restricted data exposed, concealment, deliberate circumvention	HR under existing process	Per disciplinary policy

Self-reported mistakes in the first [90] days are handled as coaching. Concealment is handled at step 4.

Acknowledgement

I have read and understand the [Company Name] AI Acceptable Use Policy and agree to follow it.

Name: _____	Signature: _____	Date: _____

Changes log

Version	Date	Change	Approved by
[v1.0]	[Date]	[Initial policy]	[Role]

Customization checklist

- ☐ Definition of AI tool includes recorders, extensions, agents and embedded features
- ☐ Register names every tool in use, with tier and owner
- ☐ Data classes defined with examples your team recognizes
- ☐ Personal accounts are Tier 3, with the reason written down
- ☐ Contractors and interns named in the scope
- ☐ Approval request has five fields and a response time
- ☐ Disclosure rule covers customer deliverables
- ☐ Enforcement steps point to your disciplinary process
- ☐ Reporting is safe: no-blame window and no-retaliation line
- ☐ Someone owns the register and the review date
- ☐ Every bracket is filled in
- ☐ Counsel or HR has read it

Free template from ComplyJet, https://www.complyjet.com/blog/ai-acceptable-use-policy. A starting point, not legal advice. Review by counsel or your HR lead is recommended before use.