CurrentWare

AI TOOLKIT • ENTERPRISE EDITION

AI Acceptable Use Policy Template

A ready-to-edit policy for organizations that sets out which AI tools employees can use, what information they can share, who governs AI decisions, and how AI use stays visible and auditable.

POLICY OWNER [Name, Title]	APPROVED BY [AI Governance Committee]	CLASSIFICATION [Internal]
EFFECTIVE DATE [Date]	VERSION [1.0]	NEXT REVIEW [Date]

HOW TO USE THIS TEMPLATE

Replace every item in [red brackets] with your organization's details, delete any clauses that do not apply, and have legal or HR review the final version before you distribute it. This template is a starting point, not legal advice.

SECTION 01

Purpose

[Company Name] supports the use of artificial intelligence (AI) tools that help employees work more effectively. This policy sets out how AI tools may be used for work so that the organization can benefit from them while protecting company data, clients, and employees.

SECTION 02

Scope

This policy applies to:

- All employees, contractors, and temporary staff of [Company Name], including all subsidiaries, regions, and business units.
- Third parties, vendors, and partners who use AI to process [Company Name] data.
- Any AI tool used for company work, whether accessed through a company account or a personal one.
- Company-owned devices and any personal devices used for company work.
- AI features built into other software, such as email, document, and meeting tools.
- AI agents, plugins, and API integrations that connect to company systems or data.

SECTION 03

Definitions

AI tool	Any software that generates text, images, code, audio, or analysis using artificial intelligence, including AI features inside other products.
Approved AI tool	A tool listed in Section 07 and accessed through a company-managed account.
Shadow AI	Any AI tool used for work without IT approval, including personal accounts on approved tools.
Sensitive information	Confidential or restricted data as defined in Section 12, including personal information, client data, and intellectual property.

SECTION 04

Policy Approach

[Choose one approach and delete the others. You can set a different approach for individual teams.]

Restrictive	Only the AI tools listed in Section 07 may be used. All other AI tools are blocked on company devices and networks.
By Approval	Approved tools may be used freely. Other tools must be requested and reviewed under Section 08 before use is approved.
Open With Monitoring	Employees may use any AI tool, provided they follow Sections 11 and 12. All AI use is monitored under Section 13.

SECTION 05

Governance And Accountability

[Company Name] governs AI through an AI governance committee with members from IT, security, legal, privacy, compliance, HR, and each major business unit.

EXECUTIVE SPONSOR	COMMITTEE CHAIR	MEETS
[Name, Title]	[e.g. CISO or CIO]	[Quarterly]

THE COMMITTEE

- Approves this policy and the approved AI tool list
- Decides on high-risk AI use cases under Section 10
- Reviews monitoring reports, incidents, and adoption metrics
- Reports AI risk to [executive leadership / the board] [quarterly]

SECTION 06

Regulatory And Framework Alignment

This policy supports compliance with the laws and standards below. [Keep those that apply and add any industry-specific requirements.]

GDPR / UK GDPR	EU AI Act	CCPA / CPRA	PIPEDA
HIPAA	NIST AI RMF	ISO/IEC 42001	SOC 2 / ISO 27001

SECTION 07

Approved AI Tools

The following tools are approved for work use when accessed through a company-managed account. IT maintains the current list at [intranet link].

AI tool	Approved for	Highest data level allowed	Notes
[e.g. Microsoft Copilot]	[All staff]	[Internal]	
[Tool name]	[Team]	[Level]	
[Tool name]	[Team]	[Level]	
[Tool name]	[Team]	[Level]	

SECTION 08

Requesting A New AI Tool

Employees who need a tool that is not on the approved list should request it rather than use it without approval.

01
Submit request
Describe the tool, the task, and the data involved.

02
Security review
IT checks data handling, storage, and vendor terms.

03
Pilot
A small group tests it against a benchmarked workflow.

04
Decision
The tool is approved, restricted, or kept under review.

Submit requests to [email or ticketing system]. Target response time: [10 business days].

SECTION 09

Vendor And Tool Requirements

Before any AI tool is approved or purchased, procurement and IT confirm that it meets these minimum requirements.

- ✓ Enterprise agreement and data processing agreement in place
- ✓ SSO and automated user provisioning
- ✓ Data retention and deletion controls
- ✓ Independent security certification, such as SOC 2 Type II or ISO 27001
- ✓ Company data is not used to train vendor models
- ✓ Admin controls and audit logs available to IT
- ✓ Data stored in approved regions **[list regions]**
- ✓ Defined security incident notification process

AI AGENTS AND INTEGRATIONS

Agents, plugins, and API connections that can read or act on company systems require a separate security review, even when the underlying AI tool is approved.

SECTION 10

Use-Case Risk Tiers

TIER	EXAMPLES	REQUIREMENT
Low	Drafting, summarizing, and research using public or internal information.	**Approved tools only. No further review required.**
Medium	Work with confidential data, or output shared with clients.	**Manager approval and human review of all output required for use.**
High	Decisions about employment, credit, health, or legal rights; automated actions on production systems.	**AI impact assessment and committee approval required before use. Periodic audits recommended.**

SECTION 11

Acceptable And Prohibited Use

EMPLOYEES MAY

+ Draft, summarize, and edit documents and emails
+ Research topics and brainstorm ideas
+ Write, review, and debug code in approved coding tools
+ Analyze data within the limits set in Section 12
+ Automate repetitive tasks and workflows

EMPLOYEES MAY NOT

– Enter confidential or restricted information into unapproved tools
– Use personal AI accounts for company work
– Make final decisions about hiring, pay, or discipline based on AI output alone
– Present AI-generated work to clients without human review and revision
– Use AI to create harassing, discriminatory, or misleading content
– Connect AI agents, plugins, or integrations to company systems without approval
– Bypass or disable monitoring or access controls set by the organization

Responsibility for AI output

Employees are responsible for any work they produce with AI. Please remember to always check AI output for accuracy, bias, and copyright concerns before using or sharing it externally. Where [Company Name] requires it, you must disclose that AI was used in the creation of the output.

TEAM-SPECIFIC RULES

[Optional: add any additional rules for teams with stricter information-handling duties, such as legal, finance, or healthcare.]

SECTION 12

Data Handling

What employees may enter into an AI tool depends on the type of information and whether the tool is approved. When in doubt, treat information as confidential.

Data level	Examples	Approved tools	Unapproved tools
Public	Published marketing content, public website text	**Allowed**	**Allowed**
Internal	Internal procedures, meeting notes, non-sensitive drafts	**Allowed**	Not allowed
Confidential	Client data, financials, contracts, source code	**Only if listed for this level**	Not allowed
Restricted	Personal information, health records, passwords, regulated data	Not allowed	Not allowed

[Align these levels with your existing data classification policy.]

If sensitive information is shared by mistake

01 Stop using the tool for that task.

02 Delete the conversation or file from the tool where possible.

03 Report it to [IT / security contact] within [24 hours].

Reporting a mistake promptly will not, on its own, lead to disciplinary action.

SECTION 13

Monitoring

[Company Name] monitors AI use on company devices and networks to find Shadow AI, enforce this AI Acceptable Use Policy, and measure adoption of approved tools. Monitoring may include reviewing which AI platforms are accessed, who is accessing them, from which devices they are being accessed, and active time. Findings are reported to the AI governance committee [quarterly]. Monitoring is carried out in line with [applicable privacy laws in your jurisdiction and the current employee monitoring policy].

SECTION 14

Roles And Responsibilities

Executive Sponsor	Owns AI risk at the leadership level and approves this policy.
AI Governance Committee	Maintains the approved list, decides on high-risk use cases, and reviews monitoring reports.
Employee	Follows this policy, completes training, requests new tools, and reports mistakes.
Manager	Makes sure their team understands the policy, ensures policy adherence, and flags any new tool requests.
IT And Security	Maintains the approved list, reviews new requests, and manages each level of access and monitoring, by team, and for the whole organization.
Legal, Compliance, HR	Reviews the policy, advises on data and privacy concerns, and handles any serious or repeat policy violations.
Procurement	Confirms vendor requirements in Section 09 are met before any AI purchase decisions are made.
Internal Audit	Tests compliance with this policy on a [bi-annual] basis.

SECTION 15

Training And Awareness

All staff must complete the AI acceptable use training within **[30 days]** of joining and repeat training **[annually]** after that. Teams that handle confidential or restricted data must also complete additional role-specific training. **[HR / learning platform]** tracks completion.

SECTION 16

Exceptions

Exceptions must be requested in writing to the AI governance committee, with the business reason, risks, compensating controls, and an end date. Exceptions last no longer than **[12 months]** and are recorded in an exception register.

SECTION 17

Records And Retention

Prompts and outputs used in business decisions are considered business records. They are kept according to **[records retention schedule]** and are subject to legal hold and e-discovery.

SECTION 18

Violations

Violations may result in loss of access to AI tools and disciplinary action up to and including termination, in line with **[HR policy]**. Violations involving personal or regulated data follow the appropriate **[incident response plan]**.

SECTION 19

Policy Review

The AI governance committee reviews this policy at least **[every six months]**, and sooner after a major regulatory change or following an incident. The approved tool list is reviewed and updated as needed.

RELATED POLICIES

[Information Security Policy, Data Classification Policy, Privacy Policy, Employee Monitoring Policy, Records Retention Schedule, Incident Response Plan, Vendor Risk Management Policy]

SECTION 20

Employee Acknowledgement

I have read and understood the **[Company Name]** AI Acceptable Use Policy. I agree to follow it, and I understand that AI use on company devices and networks is monitored and regulated.

EMPLOYEE NAME

DEPARTMENT

SIGNATURE

DATE

Need help putting this policy into practice?

CurrentWare

BrowseReporter shows which AI tools are in use. **BrowseControl** manages access by team.

NEW CLIENTS
sales@currentware.com

EXISTING CLIENTS
success@currentware.com

TECHNICAL SUPPORT
support@currentware.com

1-888-912-9619

Sales: **Ext. 1** Technical Support: **Ext. 2**