OSIbeyond ONE

AI Acceptable-Use Policy Template

A policy your leadership can approve as written, a one-page summary for staff, and a checklist of the controls that make it stick.

Version 1.0 · September 2026 · Prepared by OSIbeyond

How to Use This Template

Most organizations haven't adopted AI. Their employees have. Documents, customer or member records, and financial data are already going into consumer AI tools that nobody approved, usually with no policy, no visibility, and no controls. This template gets a policy in place quickly so the organization decides how AI is used, rather than discovering how it has been used.

The template has three parts:

- **The policy** (Part 1). Written for a leadership team to approve as-is. Replace the bracketed fields, delete any section that doesn't apply, and sign.
- **The one-page staff summary** (Part 2). What every employee needs to know, in plain language. Circulate it with the policy.
- **The control checklist** (Part 3). A policy nobody can enforce isn't a policy. This maps each rule to the control that enforces it, so you can see where the gaps are.

Fields to replace appear like this: **[Organization Name]**. A search for "[" will find them all.

> **A note on legal review.** This template reflects common practice for organizations of 10–200 staff. It is not legal advice. Regulated industries, organizations handling health or payment data, and organizations with union or contractual obligations should have counsel review the final policy before adoption.

Part 1 — Acceptable Use of Artificial Intelligence Tools

Organization	
Policy owner	
Technical contact	
Effective date	
Review cycle	Annually, and whenever an approved tool or the organization's data-handling obligations change

1. Purpose

This policy sets out how employees, contractors, and volunteers of **[Organization Name]** ("the Organization") may use artificial intelligence tools in the course of their work. Its purpose is to let people use AI productively while protecting the Organization's data, the people it serves, and its reputation.

2. Scope

This policy applies to everyone who works on behalf of the Organization and to every AI tool used for work, whether the Organization provides it or an individual signs up for it. It covers general-purpose assistants (chat, writing, and coding tools), AI features embedded in productivity software, browser extensions, meeting recorders and transcription services, image and audio generators, and any service that sends the Organization's information to a third party for AI processing.

3. Definitions

- **Approved AI tool.** A tool the Organization has reviewed, licensed or enabled, and listed in Appendix A. Approved tools are configured so that the Organization's data is not used to train the vendor's models and is retained under the Organization's control.
- **Consumer AI tool.** A publicly available AI service used under a personal or free account, or under terms the Organization has not reviewed.
- **Confidential information.** Anything not intended for the public: personal information about staff, customers, members, donors, or clients; financial and payment data; contracts and pricing; credentials; internal communications; and any information covered by a legal, regulatory, or contractual obligation. See Section 5.

4. Permitted Use

Employees may use approved AI tools for work, including drafting and editing, summarizing documents the Organization owns, research, brainstorming, meeting notes, data analysis on non-confidential data, and writing or reviewing code, subject to the rules in this policy.

Employees may use consumer AI tools for work only with public or non-sensitive information (Section 5, Level 1), and only where the tool is not blocked by the Organization's controls. When in doubt, use an approved tool or ask the technical contact.

5. Information That May Be Used With AI Tools

Level	Examples	Rule
1 **Public**	Published content, marketing copy, public event details, general knowledge questions	May be used with any tool that is not blocked.
2 **Internal**	Internal drafts, meeting notes without personal details, process documents, non-sensitive reports	Approved AI tools only.
3 **Confidential**	Personal information, customer/member/donor records, financial data, contracts, pricing, legal matters, HR matters, credentials, security details	Approved AI tools only, and only where the tool is configured for confidential data as noted in Appendix A. Never in a consumer AI tool.
4 **Restricted**	Data the Organization is legally or contractually required to protect (e.g., health, payment card, regulated or classified information)	Not to be entered into any AI tool unless the policy owner has approved that tool for that data in writing.

If you are unsure which level applies, treat the information as Level 3.

6. Prohibited Use

- Entering Level 3 or Level 4 information into any consumer AI tool, or into an approved tool not configured for it.
- Using personal accounts for work AI tasks when an approved tool is available.
- Disabling, bypassing, or working around controls the Organization uses to manage AI tools, including web filtering and data loss prevention.
- Connecting AI tools, plug-ins, or browser extensions to the Organization's email, files, or systems without approval from the technical contact.
- Recording or transcribing meetings with AI tools without informing participants, or where recording is not permitted.
- Using AI to generate content that impersonates a real person, misrepresents the Organization, or is discriminatory, harassing, or unlawful.
- Presenting AI-generated work as reviewed fact without checking it (Section 7).

7. Accountability for AI Output

AI tools produce confident, fluent, and sometimes wrong answers. The person using the tool is responsible for the result. Before relying on or sharing AI output, verify facts, figures, citations, and legal or financial statements; review generated code before it runs; and ensure the output does not include someone else's copyrighted material or confidential information. AI assistance does not change who is accountable for a decision, a document, or a communication.

8. Transparency

When AI has materially generated content that goes to people outside the Organization, disclose it where a reasonable recipient would expect to know: **[e.g., published articles, formal reports, member or customer communications]**. Internal drafting assistance does not require disclosure.

9. Security and Incident Reporting

Approved AI tools are protected by the same security controls as the rest of the Organization's systems: multifactor authentication, managed devices, and monitoring. If confidential information is entered into an unapproved tool, if an AI tool behaves unexpectedly with the Organization's data, or if you suspect an AI-generated phishing message or impersonation, report it immediately to **[technical contact]**. Reporting a mistake promptly is always the right call and will not by itself result in discipline.

10. Training

All staff complete AI acceptable-use training at onboarding and annually, including how to recognize AI-generated phishing and impersonation, which the traditional "look for typos" guidance no longer catches.

11. Enforcement

Violations of this policy are handled under the Organization's existing conduct and disciplinary procedures. Where a violation creates a security risk, the Organization may restrict access to systems or tools while the matter is reviewed.

12. Review

The policy owner reviews this policy at least annually and whenever the approved tool list or the Organization's data obligations change. Appendix A may be updated by the policy owner without re-approval of the policy.

Appendix A — Approved AI Tools

Tool	Approved for data up to level	Account type	Notes

Approval

Approved by	Title	Date

Part 2 — One-Page Staff Summary

Using AI at [Organization Name]: What You Need to Know

You can use AI to work faster. These six rules keep the Organization, and you, out of trouble.

- **Use the approved tools.** They're listed in Appendix A of the policy. If a tool isn't on the list, ask before you use it for work.
- **Think about what you're pasting.** Public information: any tool. Internal drafts: approved tools only. Anything about a person, money, a contract, a password, or a legal matter: approved tools only, and never a free consumer tool.
- **Don't connect AI to our email or files without asking.** Plug-ins, extensions, and meeting bots all count.
- **Check the output.** AI is confident and sometimes wrong. You own what you send.
- **Tell people when it matters.** If AI wrote something that's going outside the Organization, disclose it where a reader would expect to know.
- **Report mistakes fast.** Pasted something you shouldn't have? Got a suspicious message that reads perfectly? Tell **[technical contact]** right away. Reporting is never the wrong move.

> **Why this matters.** Attackers now write phishing with AI, so the old advice about spotting typos doesn't work. And anything you paste into a free AI tool may be stored, reviewed, or used to train someone else's model. The rules above are the difference between using AI and losing control of our information.

Part 3 — Control Checklist

A policy is a statement of intent. These are the controls that make each statement true in practice. Check off what is in place today; anything unchecked is where the policy relies on trust alone.

Policy statement	Control that enforces it	In place	Gap
Consumer AI tools are not used for confidential data (Sections 5, 6)	Web and DNS filtering that blocks high-risk consumer AI tools on organization devices and networks, with an allow list for approved tools	☐	☐
Confidential information stays inside approved tools (Section 5)	Data loss prevention and sensitivity labels in Microsoft 365 or equivalent, designed to flag or stop confidential content leaving the environment	☐	☐
Approved tools don't train on our data (Section 3)	Organization licensing and tenant settings for each approved tool, documented in Appendix A	☐	☐
No unapproved plug-ins or connections (Section 6)	Administrator approval required for third-party app consent in Microsoft 365 or equivalent; browser extension management on managed devices	☐	☐
Approved tools are protected like everything else (Section 9)	Multifactor authentication and conditional access on every account; managed, encrypted devices; endpoint detection and response	☐	☐
Copilot or embedded AI only sees what it should (Section 5)	Permissions review and oversharing cleanup before enabling AI features that read across email and files	☐	☐
Staff recognize AI-generated phishing (Sections 9, 10)	Security awareness training that includes AI-written phishing and impersonation, with periodic simulations	☐	☐
Incidents are reported and handled (Section 9)	A named contact, a reporting path staff know, and monitoring that can see AI-tool traffic and data movement	☐	☐
Leadership can see how AI is being used (Section 12)	Usage reporting for approved tools and visibility into attempts to reach blocked tools; for organizations enabling Copilot broadly, governance reporting on what AI can access	☐	☐

If most of the right-hand column is unchecked, the policy is still worth adopting; it sets the expectation. But treat the gaps as the next project, not as acceptable.