VERSION 1.0 · NOVEMBER 2026

AI Use Policy template

For nonprofits and charities in the United States

Not legal advice. This template is a practical starting point, not legal advice. Using it does not by itself make your organization compliant with any federal or state law, and it can't cover every situation. Laws and official guidance change, and they differ from state to state: before you adopt your policy, check it with your own attorney, and review it at least once a year.

How to use this template

1. Replace everything in [square brackets] with your own details, and delete the options that don't apply.
2. Read the guidance notes in the shaded boxes, then delete them.
3. With a small group, fill in the approved tools list in Appendix A: someone from your programs or services, someone from fundraising or communications, someone who looks after staff or volunteers, and whoever handles privacy.
4. Take the policy to your board of directors for approval.
5. Train everyone it covers, and keep their signed acknowledgments and your training record (Appendix B).
6. Replace this cover and the footer with your own, and put the review date on the calendar.

You're free to use and adapt this template within your organization. Please keep this attribution and the source link on the template as distributed. When you adopt it as your own policy, you may replace the cover, footer and watermark with your own.

Published by Innovative Workspace (Innovative Workspace CLG, a not-for-profit company registered in Ireland, company number 775662). Written by Alexis Kouchev, Founder & Managing Director. The latest version is at www.innovativework.space/resources/ai-policy-template/#united-states

Contents

[Organization] AI Use Policy

1. Purpose
2. Who and what it covers
3. Words we use
4. Who does what
5. Approved tools, and tools we don't use
6. Uses that need approval first, and uses that aren't allowed
7. Personal information and confidentiality
8. A person checks the output
9. Being open about AI
10. AI literacy and training
11. Governance
12. If something goes wrong
13. Review
14. Related policies

Version history

Appendix A: Approved AI tools

Appendix B: Acknowledgment and training record

Appendix C: AI incident report

Appendix D: A one-page guide for staff and volunteers

Sources and further reading

Innovative Workspace · innovativework.space

Before you start

Agree on the answers to these questions first. They make the rest of the template quick to fill in.

- Who will own the policy, and who handles privacy?
- Which AI tools do people already use for work, including AI features in software you already have? Ask without blame.
- Which of your programs or services, or which kinds of information, would make a mistake with AI most harmful?
- Which privacy laws apply to you? That depends on the states where you operate, the people you serve and your sector (the guidance note in section 7).
- Who must approve the policy: your board of directors or someone else?

[Organization] AI Use Policy

Approved by	[The board of directors] on [date]
Policy owner	[Name, role]
Privacy lead	[Name, role]
Version	[1.0]
Next review	[Month and year: no more than one year after approval]

1. Purpose

1.1 We use AI tools to save time on [drafting, summarizing, translating, research and admin], so that more of our time goes to [our mission]. This policy sets out how we use them safely, lawfully and in line with our values, to protect the people we serve, our donors and supporters, our staff and volunteers, and our reputation.

1.2 It covers which AI tools we may use and for what, what must never go into them, who checks what AI produces, when we tell people that AI was involved, and how we train people, handle problems and keep this policy up to date.

2. Who and what it covers

2.1 This policy applies to everyone who uses AI tools for [Organization]: [staff, volunteers, board members, interns, contractors and consultants], on our devices or their own.

2.2 It covers every use of AI tools for our work, including:

- AI assistants and chatbots that write, summarize, translate or answer questions;
- AI features in software we already use, such as email, documents, video calls, meeting transcription, our donor database or our case management system;
- AI tools for images, audio and video;
- AI agents and automations that act for us, for example by sending messages or updating records.

2.3 It doesn't cover [spelling and grammar checkers that don't use generative AI]. [Delete this clause if you make no exceptions.]

> **Guidance.** Many AI features now arrive switched on in software you already use, such as meeting transcription or email summaries. List those too, not only new tools.

3. Words we use

- **AI tool:** software that uses artificial intelligence to create text, images, audio, video or code, or to make predictions, recommendations or decisions.
- **Approved tool:** an AI tool on our approved tools list (Appendix A), used through an [Organization] account, for the tasks the list approves it for.
- **Public AI tool:** any AI tool or account that we haven't approved for the task, including free and personal accounts. We have no contract with its provider that controls how it uses or keeps what we put into it.
- **Personal information:** any information about a person who can be identified, such as a name, contact details, a photo, a voice recording or a case note. Information about a person can still be personal information when it is public.

Innovative Workspace | innovativework.space

- **Sensitive information:** personal information that needs extra care, such as health information, Social Security and other government ID numbers, financial account details, immigration status, information about children, and information about a person's race or ethnicity, religion, sex life or sexual orientation, or biometrics.
- **Confidential information:** our own information that isn't public, and information that partners, funders or others gave us in confidence.

4. Who does what

- **[The board of directors]** approves this policy, oversees the risks of AI to our organization and to the people we serve, and receives a report on our use of AI at least once a year.
- **The policy owner, [name, role],** keeps this policy and the approved tools list up to date, approves new tools and uses (sections 5 and 6), keeps the training record and reports to [the board].
- **Our privacy lead, [name, role],** advises on personal information in AI tools, decides whether a privacy risk assessment is needed and handles possible data breaches. [If you are a HIPAA covered entity or business associate, name your HIPAA privacy and security officials here.]
- **Managers** make sure their teams know this policy, have done the training and use only approved tools.
- **Everyone** follows this policy, checks what AI produces and reports problems right away.

5. Approved tools, and tools we don't use

5.1 We use only the AI tools on our approved tools list (Appendix A), through [Organization] accounts, and only for the tasks the list approves them for.

5.2 Before a tool goes on the list, [the policy owner] checks, with [the privacy lead]:

- what the provider does with what we put in: whether it keeps it, for how long, and whether it uses it to train or improve its AI;
- where the information is stored and processed, and how it is protected;
- that our contract with the provider protects any personal information it processes for us (and, if HIPAA applies to us, that we have a business associate agreement before any protected health information goes into the tool);
- the settings we control, such as whether our information is used for training, chat history and who in our organization can see what;
- security: how people sign in, and that we can remove someone's access when they leave;
- whether a privacy risk assessment is needed (clause 7.5);
- accessibility, cost, and how we get our information back if we stop using the tool.

5.3 [Choose one option and delete the other.]

- **Option A:** Nobody uses a personal or free account of an AI tool for [Organization] work.
- **Option B:** Personal accounts of the tools on the approved list may be used only for [tasks], and only with information that is neither personal information nor confidential.

5.4 We don't use [AI tools whose providers use what we put in to train their AI, unless we can turn that off; AI note-takers that join calls or meetings without everyone being told; browser extensions that can read every page you open]. [Adapt this list, and record the tools you have turned down in Appendix A.]

5.5 Ask [the policy owner] before you use any other AI tool for work, including a free trial, a new AI feature in a tool we already use, or a browser extension.

Innovative Workspace · innovativework.space

Guidance. Prefer work accounts, where you control the settings and have a contract with the provider. The NIST AI Risk Management Framework (AI RMF 1.0, January 2023) and its Generative AI Profile (July 2024), from the National Institute of Standards and Technology, are voluntary guidance that can help you weigh an AI tool's risks before you adopt it. If you allow personal accounts (option B), set the conditions in writing and keep them to information that is neither personal information nor confidential.

6. Uses that need approval first, and uses that aren't allowed

6.1 **Approval first.** These uses need [the policy owner]'s written approval before they start, with a privacy risk assessment where one is needed:

- screening job or volunteer applications;
- monitoring staff or volunteers;
- assessing people's needs, or their eligibility for a service, a grant or other support;
- working with case notes or other records about the people we serve;
- putting a chatbot or AI agent in front of the public or the people we serve;
- connecting an AI tool to our systems or information, such as our donor database, case management system, shared drives or email;
- [any other use you consider high-risk].

6.2 **Not allowed.** We never use AI to:

- make a decision about a person on its own, such as who gets a service, a job, a grant or a volunteer role (clause 8.3);
- infer the emotions of staff or volunteers from their faces, voices or other biometric information;
- create realistic images, audio or video of real people without their consent;
- create intimate or sexual images of real people, or any material that sexualizes children;
- mislead people, for example by passing off AI-generated images, quotes or stories as real;
- do anything that breaks the law, our other policies or this policy.

Guidance. Some states and cities have rules for using AI or other automated tools to make, or help make, important decisions about people, for example in hiring, and more are coming into effect. New York City, for example, requires a bias audit and notices before employers use an automated employment decision tool. Check the rules where you operate and where the people you serve live before you use AI in a decision like this. Federal and state anti-discrimination laws apply to hiring and other decisions about people whether or not AI is involved. Knowingly publishing intimate images of a person without their consent, including AI-made "digital forgeries", can be a federal crime under the TAKE IT DOWN Act (2025), and child sexual abuse material, including computer-generated images, is illegal under federal law.

7. Personal information and confidentiality

7.1 We follow the privacy and data security laws that apply to us whenever personal information goes into an AI tool or comes out of one: [the privacy and data breach laws of the states where we operate or whose residents we serve] [HIPAA, if we are a covered entity or a business associate] [other federal or state rules for our sector, for example on health, education or children's records] [our contracts and grant agreements]. [Keep what applies to you.]

7.2 **Never put personal or beneficiary information into public AI tools.** Never put any of these into a public AI tool, or into an approved tool that isn't approved for them:

- names, contact details, case details, photos or recordings of the people we serve;
- health information and other sensitive information;

- information about children or vulnerable adults;
- donor, supporter, member, staff and volunteer records;
- Social Security numbers, passwords, bank details and other security information;
- anything confidential, ours or our partners' and funders'.

7.3 The only exceptions are tools that Appendix A approves for that kind of information, after a privacy risk assessment where one is needed.

7.4 Even in an approved tool, use as little personal information as the task needs. Remove names and other identifying details where you can, and remember that removing a name doesn't always make information anonymous: other details can still identify someone.

7.5 [The privacy lead] decides whether a use of AI needs a privacy risk assessment (or the data protection assessment that some state laws require) and, if it does, completes it before the tool is used.

7.6 Our privacy notice tells people how we use their personal information, including when AI tools process it. Requests from people about their information cover what is in our AI tools too.

> **Guidance: which privacy laws apply (November 2026).**
>
> - There is no single national privacy law for nonprofits: most rules come from the states, and from federal laws for particular sectors. The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act, is one example of a state law: California's Attorney General says it "generally does not apply to nonprofit organizations". Other states' consumer privacy laws, such as Colorado's and Oregon's, can also apply to nonprofits that meet their thresholds. Check the laws where you operate and where the people whose information you handle live.
> - **HIPAA** applies only to covered entities (health plans, health care clearinghouses and health care providers that conduct certain transactions electronically) and their business associates. If it applies to you, protected health information may go into an AI tool only where HIPAA permits it, with a business associate agreement where one is required.
> - Even where no privacy law applies to an activity, following these rules protects the people you serve and keeps their trust.

8. A person checks the output

8.1 AI can be wrong, biased or out of date, and it can make things up, however confident it sounds. Whoever uses it checks facts, figures, names, quotes, sources and tone before anything is sent, published or acted on, and is responsible for the result.

8.2 Take extra care with anything about the people we serve, safety and well-being, money or legal matters, and with anything published in our name.

8.3 **People decide about people.** AI can help to prepare information, but a person with the right knowledge and authority makes every decision about a person, and can explain it.

8.4 Don't present AI output as a real quote, a real event or someone's own words unless it is one, and check that it doesn't copy someone else's work.

> **Guidance.** There is no single, comprehensive federal law on AI in the United States, and the NIST AI Risk Management Framework is voluntary. Federal and state policy on AI is changing quickly, including on how far states' own AI laws apply: check the current position each time you review this policy. Existing laws, such as privacy, consumer protection, civil rights and employment laws, still apply when you use AI.

9. Being open about AI

9.1 We tell people when they are dealing with an AI system rather than a person, for example a chatbot on our website, unless that is obvious.

9.2 We label realistic images, audio and video that AI has generated or altered, and we never use them to mislead.

9.3 Text we publish to inform the public is reviewed and fact-checked by [role] after any AI changes, under [Organization]'s editorial responsibility. If it isn't, we label it as AI-generated.

9.4 We tell the people we serve when AI is used in a way that affects them, in plain language, and we offer them a person to talk to instead.

9.5 We publish a summary of this policy on our website, and we follow our funders' rules on AI.

9.6 If anyone asks whether we used AI, we answer honestly.

> **Guidance.** Some states have rules, for some situations, on telling people that they are dealing with a bot or with generative AI. Check the rules where you operate before you put a chatbot in front of the public.

10. AI literacy and training

10.1 Everyone completes the AI introduction for their role before they use AI tools for us. It covers [how the tools work and where they fail, this policy, personal information, checking output, and the risks in their own work].

10.2 People whose use of AI affects the people we serve, our staff, our volunteers or our donors, such as [caseworkers, fundraisers and those who recruit or manage people], also learn the risks of their own work.

10.3 Managers and board members learn enough to oversee our use of AI and set the rules.

10.4 Everyone does a refresher when we add a tool or change this policy, and at least [once a year].

10.5 [The policy owner] keeps a record of who was trained, on what and when (Appendix B).

> **Guidance.** Training on this policy is the simplest way to make it work. If your organization has staff, volunteers, operations or people it serves in the European Union, the EU AI Act may also apply to you. Its Article 4, which has applied since February 2, 2025, and was amended in July 2026, asks organizations that use AI systems to take measures to support the AI literacy of their staff and of others who use AI on their behalf. It sets no required level and no certificate: the European Commission says organizations can keep an internal record of their training instead. The Act can reach organizations outside the EU, for example when the output of an AI system they use is used in the EU (Article 2(1)). Check with your attorney whether it applies to you.

11. Governance

11.1 [The board] approves this policy, and reviews the risks of AI [at least once a year] as part of our risk management.

11.2 [The policy owner] reports to [the board] at least once a year on the AI tools we use, new uses approved, training, incidents and complaints, and the changes needed.

11.3 Our board remains responsible for how [Organization] uses AI, including for fundraising.

Guidance. We found no federal rule that requires a charity or nonprofit to have an AI policy: IRS Form 990 asks about some governance policies, such as conflict of interest, whistleblower and document retention policies, but not about AI. Your board's usual duty to oversee the organization's risks covers AI too: a board-approved policy, a list of approved tools and a training record are a practical way to show that oversight.

12. If something goes wrong

12.1 Tell [the policy owner] and [the privacy lead] right away if:

- personal or confidential information went into a tool that isn't approved for it;
- AI output that was wrong, biased or harmful was sent, published or acted on;
- someone complains about our use of AI;
- an AI tool behaves unexpectedly or is compromised, or its provider changes its terms or settings in a way that affects us;
- you're not sure whether something was allowed.

12.2 Don't try to fix it alone, and don't delete anything. Write down what happened, when, in which tool, what information was involved and who might be affected (Appendix C).

12.3 [The privacy lead] treats personal information put into a tool that isn't approved for it as a possible data breach, and decides under our incident response procedure, with legal advice where needed, whether we must notify the people affected, a state agency or anyone else.

12.4 We learn from incidents without blame, and we change this policy, the approved tools list or our training where we need to.

Guidance. All 50 states, the District of Columbia and several US territories have laws that require notice when certain personal information is breached. Whether a law applies to a nonprofit, what counts as a breach and the deadlines depend on each state's definitions, so get advice promptly. HIPAA has its own breach notification rule for covered entities and business associates. Agree in advance who decides, so that no time is lost looking for them.

13. Review

13.1 [The policy owner] reviews this policy at least once a year, and also when we add a tool or a new kind of use, after an incident, and when the law or official guidance changes.

13.2 [The board] approves the changes, and we record them in the version history below.

13.3 Next review: [month and year].

14. Related policies

14.1 This policy works with our [privacy policy, information security policy, safeguarding or child protection policy, social media policy, complaints policy, whistleblower policy, and equal opportunity and anti-discrimination policy]. [Keep the ones you have.]

Version history

Version	Date	What changed	Approved by
[1.0]	[Date]	[First version, based on the Innovative Workspace AI Use Policy template, United States version 1.0, November 2026]	[The board]

Innovative Workspace

Version	Date	What changed	Approved by

Innovative Workspace · innovativework.space

Appendix A: Approved AI tools

[Organization]'s approved AI tools. Last updated on [date] by [name].

Tool, plan and account	Approved for	Information allowed	Checks done	Approved by, date	Review by
[Tool and plan], through [Organization] accounts	[For example: drafting and editing letters and posts; summarizing public reports]	[For example: no personal information]	[Terms; training on our information turned off; where information is stored; contract; security; risk assessment needed?]	[Name, date]	[Date]
[Tool]	[Tasks]	[Information]	[Checks]	[Name, date]	[Date]
[Tool]	[Tasks]	[Information]	[Checks]	[Name, date]	[Date]

Tools we have turned down

Tool	Why not	Decided by, date
[Tool]	[Reason]	[Name, date]
[Tool]	[Reason]	[Name, date]

Innovative Workspace · innovativework.space

Appendix B: Acknowledgment and training record

B1. Acknowledgment

Everyone the policy covers signs this before they use AI tools for [Organization].

I confirm that:

- I have read [Organization]'s AI Use Policy, version [1.0] of [date], and I understand it.
- I have completed the AI introduction for my role.
- I will use only approved AI tools, through [Organization] accounts, for the tasks they are approved for.
- I will never put personal information about the people we serve, or any other personal or confidential information, into a tool that isn't approved for it.
- I will check what AI produces before I send, publish or act on it, and I know I am responsible for the result.
- I will report incidents and concerns right away.

Name	
Role	
Signature	
Date	

B2. Training record

Name	Role	Training: title and format	Tools covered	Date	Refresher due

> **Guidance.** The record shows the measures you took; it doesn't certify anyone. A spreadsheet with the same columns works just as well.

Innovative Workspace · innovativework.space

Appendix C: AI incident report

Date and time of the incident	
Reported by, and when	
Tool and account used	
What happened	
Information involved: personal information? sensitive information? about how many people, and in which states?	
Who might be affected	
What we have done so far	
Privacy lead's assessment: a possible data breach? Must we notify the people affected, a state agency or anyone else (with legal advice)? If so, when were they notified?	
What we have changed: the policy, the approved tools list, the training	
Closed by, and when	

Innovative Workspace · innovativework.space

Appendix D: A one-page guide for staff and volunteers

Adapt these examples to your own work, then share this page with everyone the policy covers.

Fine, with an approved tool	Ask first	Never
Drafting or improving a letter, post or report with no personal details in it	Anything with personal information about the people we serve	Putting case notes, health information or donor records into a public AI tool
Summarizing a public report or our own published material	A chatbot or AI agent for the public	Letting AI decide who gets a service, a job, a grant or a role
Brainstorming ideas for an event or a campaign	Screening applications, or monitoring staff or volunteers	Making realistic images, audio or video of real people without their consent
Translating public information, then having a fluent speaker check it	Connecting an AI tool to our systems	Pasting passwords, bank details or Social Security numbers
Turning your own notes into a first draft, which you then check	A tool or AI feature that isn't on our list	Passing off AI output as a real quote, event or story

Before you use AI, ask yourself

- Is this tool on our approved list, through an [Organization] account?
- Is this task one the list approves it for?
- Is there personal or confidential information in what I'm about to put in?
- Who will check what comes out before it is used?

If you're not sure, ask [the policy owner] first.

Innovative Workspace · innovativework.space

Sources and further reading

We checked these sources in November 2026. Laws and guidance change: check the latest versions.

- National Institute of Standards and Technology, AI Risk Management Framework: the framework (AI RMF 1.0, NIST AI 100–1) and its Generative AI Profile (NIST AI 600–1). www.nist.gov/itl/ai-risk-management-framework
- California Attorney General, California Consumer Privacy Act (CCPA). oag.ca.gov/privacy/ccpa
- Colorado Attorney General, Colorado Privacy Act. coag.gov/resources/colorado-privacy-act/
- Oregon Department of Justice, Privacy law FAQs for nonprofits. www.doj.state.or.us/consumer-protection/for-businesses/privacy-law-faqs-for-nonprofits/
- US Department of Health and Human Services, HIPAA: covered entities and business associates. www.hhs.gov/hipaa/for-professionals/covered-entities/index.html
- Federal Trade Commission, Data breach response: a guide for business. www.ftc.gov/business-guidance/resources/data-breach-response-guide-business
- National Conference of State Legislatures, Security breach notification laws. www.ncsl.org/technology-and-communication/security-breach-notification-laws
- New York City Department of Consumer and Worker Protection, Automated employment decision tools. www.nyc.gov/site/dca/about/automated-employment-decision-tools.page
- US Equal Employment Opportunity Commission, Employment tests and selection procedures. www.eeoc.gov/laws/guidance/employment-tests-and-selection-procedures
- TAKE IT DOWN Act, Public Law 119–12. www.govinfo.gov/app/details/PLAW-119publ12
- For organizations with activities in the EU: Regulation (EU) 2024/1689, the Artificial Intelligence Act, Articles 2 and 4. eur-lex.europa.eu/eli/reg/2024/1689/oj
- Regulation (EU) 2026/1744, the Digital Omnibus on AI. eur-lex.europa.eu/eli/reg/2026/1744/oj
- European Commission, AI literacy: questions and answers. digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers

From Innovative Workspace:

- AI literacy training in Ireland: what Article 4 of the EU AI Act asks of nonprofits and SMEs (for organizations with activities in the EU). www.innovativework.space/blog/ai-literacy-training-ireland-article-4/

About this template

Innovative Workspace helps nonprofits and purpose-led organizations put AI to work safely, with their people rather than around them. We're a not-for-profit company ourselves.

If you'd like help: Your Own AI Starter, our four-week, fixed-price pilot on one real admin task, includes staff training and a simple AI-use policy written with you, and our AI consulting covers AI policy and governance. Neither is legal advice: we write a practical policy and flag legal questions for your attorney.

Start with a no-obligation conversation with us: www.innovativework.space/contact/ or info@innovativework.space.

Innovative Workspace innovativework space