VERSION 1.0 · NOVEMBER 2026

# AI Use Policy template

## For charities and nonprofits in Canada

**Not legal advice.** This template is a practical starting point, not legal advice. Using it does not by itself make your organization compliant with PIPEDA, a provincial privacy law or any other law, and it can't cover every situation. Laws and official guidance change: before you adopt your policy, check it with your own lawyer or privacy officer, 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 acknowledgements and your training record (Appendix B).
6. Replace this cover and the footer with your own, and put the review date in 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/#canada

# 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: Acknowledgement 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 the answers to these questions first. They make the rest of the template quick to fill in.

- Who will own the policy, and who is your privacy officer?
- 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 where you operate, who you serve and what you do (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 officer** | [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, directors, 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:** information about an identifiable individual, 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 publicly available.

Innovative Workspace · innovativework.space

- **Sensitive information:** personal information that needs extra care, such as health or financial information, information about children, and information about a person's racial or ethnic origin, religion, sexual life or sexual orientation, or biometric information.
- **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 officer, [name, role],** is responsible for how we protect personal information, advises on personal information in AI tools, decides whether a privacy impact assessment is needed and handles possible privacy breaches. [In Quebec, the person with the highest authority in the organization is responsible for the protection of personal information and can delegate that role in writing; publish the title and contact details of the person in charge on your website.]
- **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 officer]:

- 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, including outside Canada, and how it is protected there;
- that our contract with the provider protects any personal information it processes for us at least as well as we do;
- 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 impact 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.

InnovativeWorkspace · innovativework.space

**Guidance.** Prefer work accounts, where you control the settings and have a contract with the provider. Where PIPEDA applies, you remain responsible for personal information you transfer to a third party for processing, and must use "contractual or other means to provide a comparable level of protection" while it is processed (principle 4.1.3). In Quebec, before personal information is communicated outside the province, including to a provider that will hold it elsewhere, a privacy impact assessment and a written agreement are required (section 17 of Quebec's private-sector privacy law). 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 impact 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.** In Quebec, if you make a decision about someone based exclusively on automated processing of their personal information, you must tell them no later than when you tell them the decision. On request, you must also tell them the personal information used, the reasons and the principal factors and parameters that led to the decision, and their right to have that information corrected, and let them submit observations to a member of your staff who can review the decision (section 12.1). In Ontario, since January 1, 2026, employers with 25 or more employees must say in a publicly advertised job posting whether they use artificial intelligence to screen, assess or select applicants. Human rights laws, federal and provincial, forbid discrimination in employment and services, whether or not AI is involved. Since July 2026, the Criminal Code's offence of publishing an intimate image without consent also covers images made with artificial intelligence that are likely to be mistaken for a real recording of the person (section 162.1), and child sexual abuse and exploitation material is a crime however it was made (section 163.1).

## 7. Personal information and confidentiality

**7.1** We follow privacy law whenever personal information goes into an AI tool or comes out of one: [the Personal Information Protection and Electronic Documents Act (PIPEDA), for our commercial activities] [Quebec's Act respecting the protection of personal information in the private sector] [the Personal Information Protection Act of Alberta] [the Personal Information Protection Act of British Columbia] [the health information law of our province] [our contracts with funders and governments]. [Keep what applies to you.]

innovativework.space

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 Insurance Numbers, health card 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 impact 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 officer] decides whether a use of AI needs a privacy impact assessment and, if it does, completes it before the tool is used. [In Quebec, an assessment is required for any project to acquire, develop or overhaul an information system or electronic service delivery system involving personal information, and before personal information is communicated outside Quebec.]

7.6 Our privacy policy tells people how we use their personal information, including when AI tools process it. Requests from people to see or correct their personal information cover what is in our AI tools too.

> **Guidance: which privacy law applies (November 2026).** It depends on where you operate, who you serve and what you do.
>
> - **PIPEDA**, the federal private-sector privacy law, overseen by the Office of the Privacy Commissioner of Canada (OPC), covers commercial activities. The OPC says non-profit organizations "are usually not subject to" PIPEDA "because they do not typically engage in commercial activities": collecting membership fees and fundraising, for example, are not commercial. But "non-profit status does not automatically exempt an organization", and selling, bartering or leasing a list of members or donors is a commercial activity.
> - **Provincial laws** may apply instead. Quebec's private-sector privacy law can apply to a non-profit that carries on an organized economic activity, case by case. British Columbia's Personal Information Protection Act applies to non-profit organizations. Alberta's applies to some non-profits, such as those incorporated under its Societies Act, only for their commercial activities; whether a non-profit is fully covered depends on how it is incorporated. Several provinces also have laws on health information.
> - The federal, provincial and territorial privacy commissioners' principles for generative AI (December 7, 2023) ask organizations to use anonymized or de-identified information in prompts where they can, and, where personal information "must be entered into a prompt, only do so where authorised". 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.** Canada has no federal law written specifically for AI. The proposed Artificial Intelligence and Data Act, part of Bill C-27, never became law: the bill died when Parliament was prorogued on January 6, 2025. The federal Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems (2023) is voluntary, and written for the organizations that develop and manage those systems. The privacy commissioners say generative AI tools "do not occupy a space outside of current legislative frameworks", and that accountability for decisions rests with the organization, not with an automated system: your privacy, human rights, employment and other obligations still apply when you use AI. What is changing: in November 2026, bills on privacy (C-36, which would replace the privacy part of PIPEDA) and on online safety (C-34) were before Parliament. They are proposals, not law.

## 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.** The privacy commissioners' principles for generative AI ask organizations to ensure that outputs that could have a significant impact on a person are "meaningfully identified as being created by a generative AI tool". In Quebec, people affected by a decision based exclusively on automated processing must be told (the guidance note in section 6 of this policy), and if you collect personal information from people with technology that can identify, locate or profile them, you must first tell them, and how to activate those functions (section 8.1).

## 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 directors 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).

innovativework.space

> **Guidance.** Training on this policy is the simplest way to make it work. If your organization has staff, volunteers, operations or service users 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 adviser 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 directors remain responsible for how [Organization] uses AI, including for fundraising.

> **Guidance.** At the time of writing, we found no guidance on AI from the Canada Revenue Agency's Charities Directorate. A board-approved policy, a list of approved tools and a training record are a practical way for directors to show that they oversee the risks.

## 12. If something goes wrong

**12.1** Tell [the policy owner] and [the privacy officer] 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 officer] treats personal information put into a tool that isn't approved for it as a possible privacy breach, and decides under our breach procedure whether it must be reported to [the Office of the Privacy Commissioner of Canada] [Quebec's Commission d'accès à l'information] [our provincial privacy commissioner] and whether the people affected must be told.

**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.** Under PIPEDA, a breach of security safeguards involving personal information under your control must be reported to the OPC, and the people affected notified, as soon as feasible, if it is reasonable to believe that it creates a real risk of significant harm; you must keep a record of every breach for 24 months. In Quebec, a confidentiality incident that presents a risk of serious injury must be reported promptly to the Commission d'accès à l'information and to the people concerned, and every incident goes in a register. Alberta's law requires notice to its Information and Privacy Commissioner, without unreasonable delay, where there is a real risk of significant harm. Agree in advance who decides, so that no time is lost looking for them.

Innovative Workspace innovativ space

## 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 vulnerable persons policy, social media policy, complaints policy, whistleblower policy, and equity, diversity and inclusion 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, Canada version 1.0, November 2026] | [The board] |
| | | | |
| | | | |

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; privacy impact 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: Acknowledgement and training record

### B1. Acknowledgement

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?** | |
| **Who might be affected** | |
| **What we have done so far** | |
| **Privacy officer's assessment: a possible privacy breach? A real risk of significant harm (or, in Quebec, a risk of serious injury)? Reportable to [the OPC] [the Commission d'accès à l'information] [our provincial commissioner] ? If so, when was it reported? Must the people affected be told?** | |
| **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 Insurance 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.


- Office of the Privacy Commissioner of Canada, How PIPEDA applies to charitable and non-profit organizations. www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_19/
- Personal Information Protection and Electronic Documents Act (PIPEDA). laws-lois.justice.gc.ca/eng/acts/P-8.6/
- Office of the Privacy Commissioner of Canada, What you need to know about mandatory reporting of breaches of security safeguards. www.priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/gd_pb_201810/
- Principles for responsible, trustworthy and privacy-protective generative AI technologies, December 7, 2023. www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/
- Quebec, Act respecting the protection of personal information in the private sector (CQLR, c. P-39.1): sections 3.1, 3.3, 3.5 to 3.8, 8.1, 12.1 and 17. www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1
- Government of Alberta, Personal information for non-profits and other organizations. www.alberta.ca/personal-information-for-non-profits-and-other-organizations
- British Columbia, Personal Information Protection Act. www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01
- Innovation, Science and Economic Development Canada, Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems. ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems
- LEGISinfo, Bill C-27 (44th Parliament). www.parl.ca/legisinfo/en/bill/44-1/c-27
- LEGISinfo, Bill C-36 (45th Parliament). www.parl.ca/legisinfo/en/bill/45-1/c-36
- Criminal Code, section 162.1. laws-lois.justice.gc.ca/eng/acts/C-46/section-162.1.html
- Ontario, Requirements related to publicly advertised job postings (Employment Standards Act, 2000). www.ontario.ca/document/your-guide-employment-standards-act-0/requirements-related-publicly-advertised-job
- 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 lawyer or privacy officer.

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

Innovative Workspace · innovativework.space