VERSION 1.0 · NOVEMBER 2026

AI Use Policy template

For charities and nonprofits in the UK and Ireland

Not legal advice. This template is a practical starting point, not legal advice. Using it does not by itself make your organisation compliant with the GDPR, the EU AI Act or any other law, and it can't cover every situation. Laws and regulators' guidance change: before you adopt your policy, check it with your own adviser or data protection 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 services, someone from fundraising or communications, someone who looks after staff or volunteers, and whoever handles data protection.
4. Take the policy to your board or committee 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 diary.

You're free to use and adapt this template within your organisation. 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/#uk-ireland

Contents

[Organisation] 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 data 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 handles data protection?
- Which AI tools do people already use for work, including AI features in software you already have? Ask without blame.
- Which of your services, or which kinds of information, would make a mistake with AI most harmful?
- Who must approve the policy: your board of trustees, your management committee or someone else?

[Organisation] AI Use Policy

Approved by	[The board of trustees] on [date]
Policy owner	[Name, role]
Data protection 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, summarising, 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 support, our 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 [Organisation]: [staff, volunteers, trustees, 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, summarise, translate or answer questions;
- AI features in software we already use, such as email, documents, video calls, meeting transcription, our CRM 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 a [Organisation] 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 data:** any information about a living person who can be identified, such as a name, contact details, a photo, a voice recording or a case note. Information about a person is still personal data when it is public.

Innovative Workspace · innovativework.space

- **Special category data:** personal data about health, racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, sex life or sexual orientation, genetic data, and biometric data used to identify someone (GDPR Article 9). Information about criminal convictions and offences has strict rules too.
- **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 trustees]** approves this policy, oversees the risks of AI to our organisation 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 data protection lead, [name, role],** advises on personal data in AI tools, decides whether a data protection impact assessment is needed and handles possible data breaches. [If you have appointed a data protection officer, name them 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 straight 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 [Organisation] 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 data protection 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 data is stored and processed, and the safeguards if it leaves the UK or the European Economic Area;
- that we have a contract with the provider that covers personal data (GDPR Article 28), if the tool will process personal data for us;
- the settings we control, such as whether our data is used for training, chat history and who in our organisation can see what;
- security: how people sign in, and that we can remove someone's access when they leave;
- whether a data protection impact assessment is required (clause 7.5);
- accessibility, cost, and how we get our data 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 [Organisation] 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 data 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. Before you approve a tool, Ireland's Data Protection Commission advises that you "understand what personal data it uses, how it uses it, where the personal data goes", and whether it is "retained by the provider of the AI product or re-used in any way". If you allow personal accounts (option B), set the conditions in writing and keep them to information that is neither personal data 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 data protection impact assessment where one is required:

- 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 support;
- putting a chatbot or AI agent in front of the public or the people we support;
- connecting an AI tool to our systems or data, such as our CRM, 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 volunteering role (clause 8.3);
- infer the emotions of staff or volunteers from their faces, voices or other biometric data, except where the system is intended for medical or safety reasons;
- create realistic images, audio or video of real people without their consent;
- create intimate or sexual images of real people, or any material that sexualises 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 the EU, the AI Act has banned some practices since 2 February 2025, among them emotion recognition at work, except for medical or safety reasons (Article 5(1)(f)). From 2 December 2026 it also bans AI that generates realistic intimate images of identifiable people without their explicit consent, or child sexual abuse material; for organisations that use AI, the ban covers using a system for that purpose. Under the EU GDPR, people have the right not to be subject to a decision based solely on automated processing that has legal or similarly significant effects on them, with limited exceptions (Article 22); the UK has a parallel rule, rewritten by the Data (Use and Access) Act 2025 from 5 February 2026.

7. Personal data and confidentiality

7.1 We follow data protection law whenever personal data goes into an AI tool or comes out of one: [in Ireland, the GDPR and the Data Protection Act 2018, and our regulator is the Data Protection Commission (DPC)] [in the UK, the UK GDPR and the Data Protection Act 2018, and our regulator is the ICO]. [Keep what applies to you.]

7.2 **Never put personal or beneficiary data 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 support;
- health information and other special category data;
- information about children or adults at risk;

- donor, supporter, member, staff and volunteer records;
- 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 data, after a data protection impact assessment where one is required.

7.4 Even in an approved tool, use as little personal data 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 data protection lead] decides whether a use of AI needs a data protection impact assessment (GDPR Article 35) and, if it does, completes it before the tool is used.

7.6 Our privacy notice tells people how we use their personal data, including when AI tools process it. Requests from people about their data, such as to see or delete it, cover what is in our AI tools too.

> **Guidance.** The AI Act does not affect the GDPR (Article 2(7)), which keeps applying to personal data that goes into AI tools or comes out of them. Ireland's Data Protection Commission says an organisation using an AI product that relies on personal data "could be a data controller and if so a formal risk assessment should be considered", and warns against relying on AI outputs "without critical human analysis or intervention". In the UK, the ICO publishes guidance on AI and data protection, which it says is under review because of the Data (Use and Access) Act 2025.

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 support, safeguarding, health and safety, 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.** In England and Wales, the Charity Commission says decision-making should not be "delegated to AI or based on AI generated content alone". For fundraising in England, Wales and Northern Ireland, the Fundraising Regulator asks for "a process for a person to check the accuracy, fairness and legality of any content generated by AI before using it".

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 [Organisation]'s editorial responsibility. If it isn't, we label it as AI-generated.

9.4 We tell the people we support 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.** In the EU, the AI Act's transparency rules (Article 50) have applied since 2 August 2026. A chatbot must let people know they are dealing with AI, unless that is obvious; that is its provider's duty, and if you had one built and run it under your own name, the provider may be you. If you use AI to create deep fakes, AI-generated or manipulated images, audio or video that resemble real people, places or events and would falsely appear authentic, you must disclose them. AI-generated or manipulated text that you publish to inform the public on matters of public interest must be disclosed too, unless it has had human review or editorial control and a person or organisation holds editorial responsibility for it. In the UK, the Fundraising Regulator says not every use of AI needs a label, but "the greater the risk of misleading donors, the more transparent you should be", and it recommends publishing your AI policy.

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 data, checking output, and the risks in their own work].

10.2 People whose use of AI affects the people we support, 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 trustees 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.** Article 4 of the EU AI Act has applied since 2 February 2025. As amended in July 2026, it asks organisations 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 organisations can keep an internal record of their training instead. It applies where the AI Act applies to you: to organisations in the EU, and it can reach UK organisations too, for example when the output of an AI system they use is used in the EU (Article 2(1)). Training on this policy can be one of your measures, and it is the simplest way to make the policy work.

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 register.

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 trustees remain responsible for how [Organisation] uses AI, including for fundraising.

Innovative Workspace

Guidance: what charity regulators say (November 2026).

- **England and Wales.** The Charity Commission said in April 2024 that it did not expect to write specific guidance on AI. It encouraged trustees to consider whether "having an internal AI policy would be beneficial", and said decision-making should not be "delegated to AI or based on AI generated content alone". Its Charity Sector Risk Assessment 2026 says trustees "remain responsible for ensuring that appropriate safeguards, oversight and risk management are in place". The voluntary Charity Governance Code (2025 edition) lists "a policy for the use of technology and AI tools" among its suggested evidence of good governance.
- **Ireland.** At the time of writing, we found no guidance on AI as such from the Charities Regulator. Start from its Charities Governance Code and its guidance for trustees.
- **Fundraising in England, Wales and Northern Ireland.** The Fundraising Regulator asks charities to "develop and agree an AI policy before using any AI tools to support your fundraising", recommends publishing it, and says trustees are "ultimately accountable" for their charity's AI use for fundraising.
- **Scotland and Northern Ireland.** Check what your own charity regulator has published: the Scottish Charity Regulator (OSCR), or the Charity Commission for Northern Ireland.

12. If something goes wrong

12.1 Tell [the policy owner] and [the data protection lead] straight 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 data protection lead] treats personal data put into a tool that isn't approved for it as a possible data breach, and decides under our data protection procedure whether it must be reported to [the DPC] [the ICO] 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 the GDPR and the UK GDPR, a personal data breach must be reported to the regulator without undue delay and, where feasible, not later than 72 hours after you become aware of it, unless it is unlikely to result in a risk to people's rights and freedoms (Article 33). The people affected must be told if the risk to them is high (Article 34). 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 regulators' 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].

innovativework.space

14. Related policies

14.1 This policy works with our [data protection policy, information security policy, safeguarding policy, social media policy, complaints policy, whistleblowing policy, and equality, 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, version 1.0, November 2026]	[The board]

Innovative Workspace · innovativework.space

Appendix A: Approved AI tools

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

Tool, plan and account	Approved for	Data allowed	Checks done	Approved by, date	Review by
[Tool and plan], through [Organisation] accounts	[For example: drafting and editing letters and posts; summarising public reports]	[For example: no personal data]	[Terms; training on our data turned off; where data is stored; contract; security; DPIA needed?]	[Name, date]	[Date]
[Tool]	[Tasks]	[Data]	[Checks]	[Name, date]	[Date]
[Tool]	[Tasks]	[Data]	[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 [Organisation].

I confirm that:

- I have read [Organisation]'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 [Organisation] accounts, for the tasks they are approved for.
- I will never put personal data about the people we support, 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 straight 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 data? special category data? about how many people?	
Who might be affected	
What we have done so far	
Data protection lead's assessment: a possible personal data breach? Reportable to [the DPC] [the ICO]? 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 data about the people we support	Putting case notes, health information or donor records into a public AI tool
Summarising 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 or bank details
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 a [Organisation] 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.

- Regulation (EU) 2024/1689, the Artificial Intelligence Act: Articles 2, 4, 5 and 50. 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
- Regulation (EU) 2016/679, the General Data Protection Regulation: Articles 9, 22, 28, 33, 34 and 35. eur-lex.europa.eu/eli/reg/2016/679/oj
- European Commission, guidelines on the transparency obligations under Article 50 of the AI Act. digital-strategy.ec.europa.eu/en/policies/guidelines-ai-transparency-obligations
- European Commission, AI literacy: questions and answers. digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
- Data Protection Commission (Ireland), AI, large language models and data protection. www.dataprotection.ie/en/dpc-guidance/blogs/AI-LLMs-and-Data-Protection
- AI Office of Ireland, national competent authorities. aioffice.gov.ie/national-competent-authorities/
- Charities Regulator (Ireland), guidance on managing a charity. www.charitiesregulator.ie/en/guidance/managing-a-charity/general
- ICO, guidance on AI and data protection. ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/
- Data (Use and Access) Act 2025, section 80 (automated decision-making). www.legislation.gov.uk/ukpga/2025/18/section/80
- Charity Commission for England and Wales, Charities and artificial intelligence, 2 April 2024. charitycommission.blog.gov.uk/2024/04/02/charities-and-artificial-intelligence/
- Charity Commission for England and Wales, Charity Sector Risk Assessment 2026. www.gov.uk/government/publications/charity-sector-risk-assessment-2026/charity-sector-risk-assessment-2026
- Fundraising Regulator, guidance for using artificial intelligence in fundraising. www.fundraisingregulator.org.uk/about-fundraising/resources/guidance-using-artificial-intelligence-fundraising
- Fundraising Regulator, new guidance to support charities using AI in fundraising. www.fundraisingregulator.org.uk/about-fundraising/resources/new-guidance-support-charities-using-ai-fundraising
- Charity Governance Code, 2025 edition. www.charitygovernancecode.org/

From Innovative Workspace:

- An AI policy template for nonprofits and NGOs in Ireland, the UK and the EU: what each part of a policy is for, and the rules behind it. www.innovativework.space/blog/ai-policy-template-nonprofits/
- AI literacy training in Ireland: what Article 4 of the EU AI Act asks of nonprofits and SMEs. www.innovativework.space/blog/ai-literacy-training-ireland-article-4/

About this template

Innovative Workspace helps nonprofits and purpose-led organisations 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 adviser or data protection officer.

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

Innovative Workspace · innovativework.space