

AI Policy Template

[CLIENT NAME]

Effective Date: [Insert Date]

Last Reviewed: [Insert Date]

1. Purpose and Scope

This Artificial Intelligence (AI) Policy establishes clear, ethical, and responsible guidelines for the use of AI technologies within [CLIENT NAME]. As generative AI tools like ChatGPT, Claude, Copilot, Gemini, Confer and others become increasingly integrated into professional workflows, this policy ensures that their use aligns with our mission, values, legal obligations, and commitment to data privacy and equity.

The purpose of this policy is to:

- Promote the safe, ethical, and effective use of AI.
- Protect the confidentiality of staff, clients, donors, partners, and organizational data.
- Mitigate risks related to bias, misinformation, and intellectual property.
- Foster transparency and accountability in AI-assisted work.

This policy applies to all employees, contractors, volunteers, board members, and third parties who use AI tools on behalf of [CLIENT NAME] whether on organizational devices or personal devices, when conducting organization-related work.

2. What is Artificial Intelligence (AI)?

Artificial Intelligence (AI) refers to systems that simulate human intelligence processes, such as learning, reasoning, problem-solving, and decision-making. In practice, AI systems analyze large datasets to identify patterns, generate insights, and produce content—including text, images, code, and audio.

Generative AI (GenAI) is a subset of AI that creates new content in response to user prompts. Tools like ChatGPT, Gemini, and Claude are examples of generative AI that use large language models (LLMs) trained on vast amounts of publicly available data.

While these tools can enhance productivity and creativity, they are not infallible. Users must understand that AI-generated content may be inaccurate, outdated, biased, hallucinated (i.e., fabricated information presented as fact), or create images that infringe on copyrights without noting where the image came from.

3. Approved AI Tools and Vendors

The following AI tools have been reviewed and approved for use within the organization:

- [Insert name of enterprise AI chatbot [CLIENT NAME] wants to use. [CLIENT NAME] should use their work email to sign-in]
- Options include: ChatGPT (already used by many at [CLIENT NAME]), Claude, Gemini, Co-Pilot
- Any other tools that are approved

“ **Note:** If you want to use any other AI tools for your personal use, you can sign up for them with your personal email. No [CLIENT NAME] data should be shared on those tools.

Any new AI tool must be reviewed by the Operations Team and approved before use.

4. Sanctioned (Approved) Uses of AI

The following uses of AI are approved when conducted in accordance with this policy and applicable data protection guidelines:

- **Brainstorming and ideation:** Using AI to generate initial ideas for reports, campaigns, or content outlines.
- **Drafting and editing:** Requesting suggestions for rewording sentences, improving grammar, or structuring paragraphs—without inputting sensitive content.
- **Research support:** Using AI to summarize publicly available information or suggest research angles (always ask the AI to cite its sources and then verify those sources).
- **Formula assistance:** Seeking help with Excel formulas (e.g., "How do I calculate average cost per unit in Excel?").
- **Content inspiration:** Brainstorming ideas for blog post outlines, social media headlines, or presentation structures—provided final content is human-reviewed and original.

All AI-assisted work must be reviewed by a person consistent with [CLIENT NAME]'s voice and standards.

5. Unsanctioned (Prohibited) Uses of AI

The following uses of AI are strictly prohibited:

- **Inputting confidential or sensitive information, including:**
 - Personal Identifiable Information (PII) such as names, addresses, SSNs, or health data.
 - Donor, client, or staff records.
 - Draft contracts, legal documents, or financial reports.
 - Proprietary code, internal strategies, or unpublished research.
 - Immigration or legal status.
 - [CLIENT NAME] financial information.
 - Employee records.
 - CVs.
- Submitting AI-generated content as final work without human review, editing, and verification.
- Using AI for hiring or employment decisions, including resume screening, candidate evaluation, or generating feedback on job applicants.
- Creating legal filings, policy documents, or compliance materials without attorney or leadership review.
- Generating content that could be offensive, discriminatory, or harmful, especially toward marginalized communities.
- Violating intellectual property rights, including uploading copyrighted materials (e.g., books, articles, music) into AI tools.
- Using AI to bypass security protocols or circumvent organizational policies.

“ **Remember:** Anything shared into a public AI becomes publicly available information and can be used to target the organization if that company is ever subpoenaed.

6. Data Privacy and Security Requirements

AI tools often store and use user inputs to improve their models. Therefore, data privacy is paramount.

Employees must:

- Never enter PII, confidential data, or sensitive organizational information into any AI system.
- Treat all AI inputs as potentially public—if you wouldn't publish it in a newspaper, don't type it into AI.
- Use only approved tools that meet our security standards (see Section 4).
- Immediately report any suspected data breach or unauthorized disclosure involving AI tools to the IT Department.

[CLIENT NAME] adheres to strict data governance principles, including:

- **Data minimization:** Collect and use only the data necessary.
 - **Encryption:** Ensure data is encrypted in transit and at rest (which it is on all AI platforms).
 - **Access control:** Limit data access based on role and necessity (principle of least privilege).
-

7. Quality Control and Verification

AI-generated content is not a verified source of information.

All AI-assisted work must undergo:

- Fact-checking against reliable, authoritative sources.
- Human review for accuracy, tone, and alignment with organizational messaging.
- Bias screening—especially for content related to race, gender, disability, or other protected characteristics.
- Editorial oversight—final approval by a supervisor or designated staff member.

“ **Staff are reminded:** You are responsible for the final product, regardless of AI involvement. Relying solely on AI output without verification is unacceptable.

8. Bias and Equity Considerations

AI systems reflect the biases present in their training data, which can perpetuate historical and societal inequities.

Employees must:

- Be aware that AI may generate biased, stereotypical, or exclusionary content.
- Actively review outputs for fairness, inclusivity, and cultural sensitivity.

- Seek diverse perspectives when evaluating AI-assisted work, especially for content affecting vulnerable
-