nten

Generative AI Use Policy

A TEMPLATE FOR ORGANIZATIONS
2024

AN NTEN GUIDE
by Nolwenn Godard &
Lindsey Washburn

What's Inside

Introduction

POLICY DISCLAIMER

This Generative AI Use Policy Template is designed to provide organizations with a framework for ethical, responsible, and transparent AI governance. It is meant to serve as a template and should be reviewed and revised based on your organization's specific needs and use of artificial intelligence technologies.

Please note that this policy template is not intended to be a legal document. You should consult with an attorney for guidance on the laws and regulations applicable to your organization.

By using all or part of the template, you agree to this disclaimer and acknowledge that the Generative AI Use Policy Template does not constitute legal advice.

HOW TO USE THIS POLICY

Organizations in the social sector are increasingly adopting generative AI to leverage the technology's ability to streamline operations, analyze data, and other use cases. With the increased usage of generative AI comes the need for guidance on the ethical and responsible use of the technology to help organizations enhance their work without compromising their values or mission. In particular, organizations in the social sector may greatly care about the privacy of their stakeholders (clients, employees, contractors), their reputation, their claim of copyright to material they produce, and their values. They need to understand how to protect these while leveraging the new technology.

To address this need, NTEN developed the following Generative AI Use Policy Template. This template aims to provide a comprehensive framework for organizations based on best practices for responsible AI. It is designed to be a living document and should be customized to address your organization's specific needs, values, and risk tolerance.

We also recommend incorporating this policy into your other existing policies, especially related to data and privacy. Find additional policy templates and examples like these in **NTEN's Publications**.

Due to the rapidly evolving nature of this technology, we encourage you to periodically (at least annually) review and revise the template to ensure the responsible use of generative AI in your organization.

By adopting this template, your organization can demonstrate its commitment to responsible AI and maintain the integrity of your mission-driven work.

ABOUT NTEN

We are creating a world where missions and movements are successful through the skillful and equitable use of technology.

We build transformative power by connecting people who are putting technology to work for social change. We strengthen their individual and collective capacity for doing good by offering expert trainings, researching effective approaches, and providing places where relationships can flourish. We relentlessly advocate for the redesign of the systems and structures that maintain inequity.

NTEN reports support the growth and development of the sector through benchmarking the technology goals and challenges of nonprofits, and by identifying areas of need.

For more, visit **nten.org/publications**.

Background and purpose

DEFINITION AND SCOPE

Generative Artificial Intelligence ("Generative AI" or "GAI") refers to a category of machine learning algorithms designed to generate text, image, video, sound, or other forms of content in response to prompts. GAI can translate, create, debug code, and generate content, including text, images, audio, and video. It can also summarize content, categorize information, and perform numerous other tasks. Several companies currently offer GAI tools.

BENEFITS AND RISKS

GAI tools have the potential to increase employee productivity, enhance innovation, and uncover new insights. However, it is crucial to recognize the risks associated with the use of GAI tools by [Your Organization] (the "Organization"). Use of these tools must be conducted responsibly and ethically, in compliance with applicable laws and vendor terms, while safeguarding the Organization's intellectual property, confidential information, and personal information of its employees, clients, volunteers, and other related personnel. This includes sensitive information such as personally identifiable information (PII), health information, financial data, and other data protected by applicable laws and regulations.

PERMISSIBLE USE

GAI tools should be used solely to further the mission and goals of the Organization. They must not be used for personal gain, unlawful activities, or any purposes that could damage the Organization's reputation.

POLICY FRAMEWORK

This policy outlines the parameters for the use of GAI tools by Organization personnel during their employment. The Organization reserves the right to amend this policy as necessary to account for new technological developments, new uses, or an increased understanding of the legal implications of using GAI.

COMPLIANCE AND ENFORCEMENT

Failure to comply with this policy may result in suspension of your access to GAI tools and/or disciplinary action.

Risks of using GAI tools

Below are seven potential risks stemming from the use of Generative AI tools in the workplace. Organization personnel using GAI tools in connection with their job responsibilities should be mindful of these risks and strive to avoid the issues described.

1. Inadvertent breach of confidentiality

Inputting information into a GAI tool may be equivalent to sharing it with a third party, depending on the tool's confidentiality capabilities and settings. Consequently, submitting confidential and/or proprietary information belonging to the Organization, its affiliates, or any of their clients, employees, or partners into a GAI tool may breach confidentiality obligations and protections, unless appropriate safeguards, such as legal terms ensuring the information's confidentiality, are in place.

2. Inadvertent breach of contract

Agreements with vendors, business partners, and other third parties may restrict the use of exchanged information to specific purposes, such as providing services or performing contractual obligations. Inputting third-party information into a GAI tool may exceed the authorized use scope under these contracts.

3. Violation of privacy laws

Submitting information qualifying as "personal data" or "personal information" into a GAI tool may constitute an impermissible use, disclosure, or sharing under the Organization's privacy policy and/or applicable privacy laws.

4. Increased cybersecurity risks

When using GAI tools to develop source code, the output may include cybersecurity vulnerabilities or other non-functional code. Integrating such code without further diligence (e.g., using third-party monitoring software tools) can introduce vulnerabilities into the Organization's codebase.

5. Intellectual property (IP) risks

Under current law, GAI-generated output is not copyright-protectable, and content in GAI output may not be considered IP owned by the Organization. Additionally, using GAI output that incorporates third-party IP (e.g., images, text, source code) without proper attribution risks infringement claims. Submitting highly sensitive trade secrets and other proprietary information into a GAI tool could irrevocably forfeit the Organization's IP rights in that information.

6. Quality and ethics of GAI output

GAI tools can produce inaccurate output (sometimes called "hallucinations") and may exhibit biases based on the data used, contrary to the Organization's values and legal obligations.

7. Environmental impact

GAI tools require significant energy to operate, resulting in a substantial carbon footprint and water consumption. The potential environmental impact of GAI should be considered as part of the risk-benefit assessment for any use case.

SCOPE

This policy applies to all staff - employees, volunteers, contractors, and any other individuals or entities engaged in activities on behalf of the Organization ("Users").

Guidelines for use of GAI tools

To address the risks described above, Organization personnel using GAI tools for work purposes shall follow the below guidelines.

WEB APP, APP, OR API USE

Before using a web app, app, or API offered by a GAI vendor, including free services, follow all relevant policies and procedures. Obtain approval from your supervisor by providing all necessary information, including the vendor's name, intended use, available terms, costs, and any other relevant details.

CONSUMER-FACING CHATBOTS

You may use GAI chatbots for simple workplace-related tasks to improve efficiency.

Attached as Exhibit A is a list of approved GAI tools for use by all Organization employees. Only these tools are approved for use. Exhibit A may be updated periodically to include new approved GAI tools. When using these tools, follow the general guidelines outlined below, as well as any specific guidelines noted for each tool in Exhibit A.

Ensure that GAI use complies with all applicable policies (in particular data privacy and security policies), laws and regulations, including those related to AI and data protection. Respect and protect intellectual property rights in the development and use of AI applications. Stay compliant with open-source licenses and all Organization policies.

Vendors must also comply with these guidelines. The Organization's procurement and external partnerships policies must specify guidelines for selecting and collaborating with GAI vendors and partners, including those with embedded GAI tools.

When using a GAI tool for professional purposes, you agree to comply with the following guidelines (as well as any additional guidelines noted for an approved GAI tool listed in Exhibit A):

1. Compliance with GAI terms and conditions

- Familiarize yourself with and adhere to the terms and policies of the GAI platform, including:
  - Restrictions on the use of outputs
  - Notice/transparency requirements for outputs
  - Attribution requirements for outputs
  - Usage guidelines, including prohibited types of inputs or uses

- For example, some GAI tools prohibit using outputs for commercial purposes. Exhibit A includes links to the terms and conditions for each approved GAI tool and highlights key provisions for review.

2. Use of corporate accounts

- Consult with your supervisor about creating or using an existing corporate account.

- If a corporate account is unavailable, create an account separate from any personal account using your work email address.

- When a corporate account is available, use it exclusively for work-related purposes.

3. Sensitive, confidential, or proprietary information inputs

- You may input commercially sensitive and confidential information into the GAI platform if authorized in Exhibit A and according to platform-specific guidelines.

- Sensitive information includes business strategy, program strategy, proprietary information, personally identifiable information, financials, and other data reasonably understood to be sensitive or confidential.

4. Personal data inputs

- Do not include employee, client, or vendor personal data in any inputs into the GAI tool unless authorized by Organization Legal.

- Where feasible, remove or anonymize personal data before uploading a file to a GAI tool.

5. Third-party data inputs

- Do not include third-party data without authorization from Organization Legal.

- Ensure that using third-party data in a GAI tool does not breach any contractual obligations. For example, vendors and business partners may restrict the use of their data to specific contractual purposes, which may not include market research or training purposes.

6. Review output for quality, accuracy, and compliance

- Ensure an Organization employee with appropriate expertise reviews the output from the GAI tool for inaccuracies, quality, and compliance issues.

- Verify against other non-GAI sources of information. Do not use or share false, misleading, or unverified information.

7. Review output for respect and fairness

- Check the output for fairness and bias. Do not use or share content that is discriminatory, harassing, or offensive.

8. Adherence to organization policies

- All Organization policies regarding confidentiality, security, and IP continue to apply when using GAI tools.

- All work product created (including inputs into and outputs from GAI tools) is the property of the Organization.

- Maintain confidentiality and follow all information security policies and protocols.

9. Communication

- Inform your supervisor if you are using a new GAI tool or using an existing tool in a new way or for a new purpose.
- If unsure about any aspect of GAI use, consult your supervisor, Organization Legal, or IT/Information Security Departments.

10. Follow the dos and don'ts for chatbots and similar AI tools

- These are outlined in Exhibit B.

Additional guidelines and best practices

ETHICAL CONSIDERATIONS

- **Fairness and bias:** Mitigate biases in GAI models and outputs. Ensure fairness across different groups.
- **Transparency:** Disclose the use of GAI to users and customers, including potential limitations. Indicate when content is AI-generated.
- **Accountability:** Establish responsibility for GAI outcomes, including error handling and remediation processes. Report any issues or negative impacts promptly.

DATA GOVERNANCE

Review and update the organization data governance policies, covering:

- **Data privacy:** Ensure privacy of internal and customer data, complying with relevant laws. Avoid reverse engineering with re-identification of anonymized data.
- **Proprietary data protection and handling:** Protect data from unauthorized access, using anonymization, encryption, and secure storage practices.
- **Data sources:** Establish policies regarding the sources of data used by GAI, including restrictions and bias considerations.

TRAINING AND AWARENESS

- **Education:** Provide regular training on responsible GAI use, including best practices, ethical considerations, and understanding GAI limitations.
- **Continuous learning:** Encourage feedback and adapt the policy as GAI technology evolves.
- **Compliance:** Ensure users complete required training and adhere to this policy.

INCIDENT MANAGEMENT

- **Reporting mechanisms:** Establishing clear procedures for reporting any issues or concerns related to GAI use.

STAKEHOLDER TRUST

- **External communication:** Set clear standards for communicating with customers and partners about AI use, terms, conditions, and responses to adverse AI outcomes.
- **Public transparency:** Make the GAI policy and its rationale publicly available on the Organization website. Include clear descriptions of permissible uses, user responsibilities, and distinctions between usage purposes.