

[Nonprofit Organization Name]

Artificial Intelligence Usage Policy

[1. Purpose](#)

[2. Scope](#)

[3. Policy](#)

[3.1. Appropriate Use of AI Systems](#)

[3.2. Identifying and Mitigating Bias in AI-generated Outputs](#)

[3.3. Ensuring Accuracy and Appropriateness of AI-generated Outputs](#)

[3.4. Data Protection and Privacy](#)

[3.5. Transparency and Accountability](#)

[3.6. Training and Awareness](#)

[3.7. Intentional Misuse](#)

[3.8. Unintentional Misuse](#)

[3.9. Reporting Misuse](#)

[3.10. AI Development and External Collaboration](#)

[3.11. Use of AI Meeting Notetakers](#)

[3.12. Ethical and Legal Use of AI Regarding Copyright](#)

[4. Enforcement](#)

[5. Review and Updates](#)

[5.1. Revision History](#)

1. Purpose

The purpose of this Artificial Intelligence (AI) Usage Policy is to establish guidelines and best practices for the responsible use of AI systems within [Nonprofit Organization Name]. The policy aims to promote the efficient and ethical use of AI tools, while minimizing the risk of intentional or unintentional misuse that may result in harm to individuals, the organization, or our mission. This policy also seeks to address potential biases, ensure alignment with the organization's mission, values, and objectives, and guarantee accuracy and appropriateness of AI-generated outputs.

2. Scope

This policy applies to all staff, volunteers, contractors, and any other individuals who have access to and use AI systems on behalf of [Nonprofit Organization Name]. The policy covers the use of AI tools and applications for work-related tasks, both on-site and remotely, including work-from-home situations.

3. Policy

3.1. Appropriate Use of AI Systems

AI systems may be used to assist in tasks such as data analysis, content creation, decision-making, and communication. Users must:

- A. Use AI tools only for their intended purpose and in accordance with any applicable laws and regulations.
- B. Ensure that AI tools are used in a manner consistent with the mission, values, and objectives of [Nonprofit Organization Name] by regularly consulting with supervisors, colleagues, and relevant stakeholders to align AI-generated outputs with organizational goals
- C. Exercise due diligence and critical thinking when using AI-generated outputs, as AI systems may produce biased, inaccurate, or inappropriate results.

3.2. Identifying and Mitigating Bias in AI-generated Outputs

To identify and mitigate potential biases in AI-generated outputs, users must:

- A. Be aware of common biases that may be present in AI systems, such as data bias, algorithmic bias, and confirmation bias.
- B. Regularly review and evaluate AI-generated outputs for potential biases and inaccuracies, seeking input from diverse perspectives and stakeholder groups.
- C. Use AI tools with transparent methodologies and documentation to better understand their decision-making processes.
- D. Collaborate with AI vendors and developers to improve AI systems and address identified biases, reporting any issues and working together to develop solutions.
- E. Document and communicate any identified biases and mitigation efforts to relevant stakeholders.

3.3. Ensuring Accuracy and Appropriateness of AI-generated Outputs

To ensure that AI-generated outputs are accurate and appropriate, users must:

- A. Verify the accuracy of AI-generated outputs by cross-checking with reliable sources, human judgment, or other relevant methods.
- B. Review AI-generated outputs for appropriateness, taking into account the context, audience, and potential impact of the content.
- C. Establish a system of checks and balances involving multiple reviewers to minimize the risk of errors or inappropriate content.
- D. Ensure that AI-generated content is properly reviewed and approved by a human before it is published or used for decision-making.
- E. Develop and implement guidelines for the responsible use of AI-generated outputs in different contexts and situations, tailored to the specific needs and requirements of [Nonprofit Organization Name].

3.4. Data Protection and Privacy

Users must adhere to [Nonprofit Organization Name]'s Data Protection Policy when using AI systems. This includes:

- A. Ensuring that sensitive and personal data is anonymized, encrypted, or otherwise protected when used with AI tools.
- B. Obtaining appropriate consent from data subjects when necessary.
- C. Reporting any data breaches or incidents involving AI systems to the designated Data Protection Officer (DPO) or other appropriate person(s).

3.5. Transparency and Accountability

Users must be transparent about the use of AI systems and accountable for the results generated by these tools. This includes:

- A. Disclosing the use of AI systems when communicating with external stakeholders, such as donors, partners, and beneficiaries.
- B. Ensuring that AI-generated content is properly reviewed and approved by a human before it is published or used for decision-making.
- C. Maintaining a record of AI tool usage, including the purpose, inputs, outputs, and any actions taken based on the AI-generated results.

3.6. Training and Awareness

All users of AI systems must undergo appropriate training to ensure the responsible and ethical use of these tools. This includes:

- A. Familiarizing themselves with this AI Usage Policy and any other relevant policies, guidelines, and best practices.
- B. Participating in regular training sessions and workshops to stay updated on AI-related developments, risks, and mitigation strategies.

3.7. Intentional Misuse

Misuse of AI systems can refer to any intentionally malicious activity that violates ethical, legal or moral standards, and compromises the safety, privacy, or security of individuals or society as a whole. Intentional misuse of AI systems is expressly forbidden. Some potential examples of intentional misuse of AI systems include:

- A. AI-based fraud: The use of AI to manipulate or cheat unsuspecting individuals or organizations through phishing scams, identity theft, or fraudulent behavior such as fraudulently issuing loans.

- B. Discrimination: AI systems may exhibit bias and perpetuate discrimination, resulting in either unequal treatment or exacerbation of existing social inequalities.
- C. Invasion of Privacy: AI systems may be used to gather personal data without the consent of individuals, leading to the violation of privacy rights.
- D. Malicious use: AI systems can be used for cyber attacks, such as phishing attempts, social engineering and vulnerability identification and exploitation.
- E. Spreading misinformation: AI systems can be used to create and distribute false or misleading information.

3.8. Unintentional Misuse

Unintentional misuse of AI systems refers to situations where users, without malicious intent, use AI tools in ways that lead to negative consequences or harm. This can occur due to a lack of understanding, insufficient training, or an oversight in the use of AI technology. Some examples of unintentional misuse include:

- A. Bias and discrimination: Users may inadvertently reinforce existing biases or discriminatory patterns present in AI-generated outputs, leading to unfair treatment of certain individuals or groups. This could occur if users are unaware of the potential biases embedded in AI algorithms or training data.
- B. Privacy violations: Users might unintentionally expose sensitive or personal information through AI systems, either by providing the AI with restricted data or by failing to anonymize or encrypt the data properly before use. This could lead to breaches of privacy regulations and harm to individuals whose data is exposed.
- C. Inaccurate or misleading information: Users may unknowingly rely on AI-generated outputs that are incorrect, outdated, or misleading, which could lead to poor decision-making, financial losses, or reputational damage for the organization.
- D. Inappropriate content: AI systems might generate content that is offensive, politically biased, or otherwise inappropriate for the intended audience or context. Users may inadvertently share or act upon such content, causing harm to the organization or its stakeholders.
- E. Over Reliance on AI: Users may unintentionally rely too heavily on AI systems, neglecting to apply their own judgment, expertise, or common sense. This could lead to the adoption of suboptimal solutions, overlooking valuable human insights, or exacerbating existing issues.

3.9. Reporting Misuse

Users are encouraged to report any suspected misuse of AI systems, whether intentional or unintentional, to their supervisor or other appropriate person(s). Reports can be made anonymously and will be handled confidentially.

3.10. AI Development and External Collaboration

When developing AI tools or engaging with external collaborators, the following guidelines must be adhered to:

- A. Collaboration agreements must clearly define the roles, responsibilities, and expectations of all parties involved. They should also address ownership and usage rights of AI models and data.
- B. All AI development and collaborations must be carried out in alignment with this AI Usage Policy, as well as any other applicable policies or guidelines of [ORGANIZATION].
- C. AI development must prioritize safety, privacy, and ethical considerations.
- D. The development process should include measures to address potential biases in AI systems, such as conducting regular bias audits, seeking diverse input, and using fair and unbiased data for model training.
- E. All external collaborators must commit to upholding the principles of transparency, accountability, and respect for privacy as outlined in this policy.
- F. Prior to deployment, AI systems should undergo rigorous testing to ensure their safety, accuracy, and reliability. They should also be reviewed for potential ethical, legal, and societal implications.
- G. AI development should include a plan for ongoing monitoring and maintenance to ensure that the system continues to operate safely and effectively, and that any new issues or concerns are promptly addressed.
- H. Any potential risks or ethical concerns related to the AI development or collaboration should be reported to the designated AI Ethics Officer or other appropriate person(s).

3.11. Use of AI Meeting Notetakers

The use of AI meeting notetakers such as fathom.video and otter.ai is permitted to facilitate accurate documentation and sharing of meeting discussions. Users must adhere to the following guidelines:

- Obtain necessary permissions from meeting participants prior to activating AI meeting notetakers.
- Ensure the accuracy of AI-generated notes by reviewing and, if necessary, editing the content.
- Abide by data privacy standards, ensuring that sensitive information is properly handled and stored.
- Notify external participants of the use of AI notetakers and provide an option for them to opt-out if desired.

3.12. Ethical and Legal Use of AI Regarding Copyright

The use of AI must honor copyright protections for authors and visual artists. Adherence to the following guidelines is required:

- Ensure that AI tools are used in a manner that respects copyright laws and ethical standards.
- Obtain necessary permissions or licenses before utilizing copyrighted materials.
- Provide proper attribution to authors and artists when using or sharing their work.
- Establish a process for reporting and addressing copyright infringements, including a designated point of contact for reporting such issues.

4. Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract, in accordance with [Nonprofit Organization Name] disciplinary procedures.

5. Review and Updates

This policy will be reviewed annually, or as needed based on changes in technology, regulation, or organizational needs. Updates will be communicated to all users and appropriate training will be provided.

5.1. Revision History

Reviewer	Date	Status	Notes
		Not started ▾	
		In progress ▾	
		Under review ▾	
		Approved ▾	