

Rhode Island Foundation

Interim Guidelines for Acceptable Use of Generative Artificial Intelligence (AI) Tools with Rhode Island Foundation Data

Introduction

Generative AI tools offer substantial benefits for creating and editing materials, donor and grantee research, and administrative operations. Potential important uses include grantmaking and impact assessments, donor relations and fundraising, operational efficiency, and community connections like matching donors to causes and trend analysis. However, their use also raises concerns about data privacy, security, and accuracy. These guidelines aim to ensure that the Foundation utilizes these tools responsibly and in compliance with legal and ethical standards.

Scope

These guidelines apply to all Foundation Team members, and any consultants, contractors, vendors, or volunteers that may have direct access to Foundation data and cover the use of generative AI tools in all Foundation-related work and activities.

Data Privacy Principles

When using generative AI tools, adhere to the following principles to protect sensitive information:

1. **Minimize Data Exposure:** Only input data that is essential for the task at hand. Do not include sensitive or confidential information.
2. **Anonymize Data:** Anonymize data by removing or altering personal identifiers.
3. **Understand Tool Capabilities:** Be aware of the data privacy and security measures of the AI tool being used. Ensure its policies align with Foundation standards and legal requirements as described in the Foundation's Acceptable Use Guidelines.

Acceptable Data Types for Input

1. **Public Information:** Data that is publicly available or intended for public dissemination. Examples include published research, public datasets, and open-source materials.
2. **Non-sensitive Internal Data:** Internal data that is not confidential or personally identifiable. Examples include publicly available marketing materials, research, and publications.

Responsibilities

1. **Users:** All Foundation Team members, and any consultants, contractors, vendors, or volunteers that may have direct access to Foundation data, are responsible for understanding and adhering to these guidelines. Users should ensure that the data they input into generative AI tools complies with the guidelines listed earlier in this document.
2. **Foundation:** The Foundation provides access to training and tools which deliver information on AI, data protection, cybersecurity, and related topics. These resources will help the Foundation's community understand generative AI tools, and the safeguards required to keep data safe. In addition, training and informational material will be distributed and updated by Rhode Island Foundation's Technology & Operations Management (T&O) Department. Any specific questions can be forwarded to the T&O Department.

Compliance

For Foundation Team members, any non-compliance with the directives outlined in this document may result in disciplinary action up to and including termination. Non-compliance with the directives of this policy by any consultants, contractors, vendors, or volunteers that may have direct access to Foundation data may result in legal action by the Foundation.

Exceptions

As of the time of publication of these guidelines, Microsoft Copilot is the only known generative AI tool designed with several features to protect data and ensure that the information processed is not uploaded to the generative AI database. Key protections include:

1. **Data Isolation:** Data input into Copilot is isolated and not used for database training or improving the service.
2. **Security Measures:** Copilot implements robust security measures to safeguard data.
3. **Compliance Standards:** The service complies with industry standards and regulations to ensure data privacy and security.

Due to these features and the fact that the standard version of Copilot is part of the Foundation's Microsoft licensing agreement and will be available to all Team members, Copilot is the only generative AI tool authorized for use.

The Chief of Staff and Chief Technology Officer will review and consider any exceptions to directives outlined within this document as needed.

Conclusion

The responsible use of generative AI tools is essential for maintaining data privacy and security. By adhering to these guidelines, the Foundation team can leverage the benefits of these technologies while upholding our commitment to ethical and legal standards.

For questions or more information about these guidelines, please contact the T&O Department via email at kmalin@rifoundation.org.

Policy Review and Revisions

Last Reviewed	Last Updated	Summary
N/A	11/06/2025	Policy created, instituted, and disseminated for signature by all Foundation Team members.