

Artificial Intelligence Acceptable Use Policy

Purpose

The purpose of this policy is to establish guidelines for the responsible, ethical, and secure use of Artificial Intelligence (“AI”) technologies within the Community Foundation for Greater Buffalo. This policy defines acceptable use of AI to enable productivity and responsible innovation while protecting our stakeholders, data, intellectual property, and reputation.

Community Foundation recognizes the transformative potential of Artificial Intelligence (AI), including generative AI tools. When used responsibly, these technologies can enhance productivity, creativity, research, operations, customer service, and decision-making. At the same time, AI tools raise important considerations related to privacy, security, bias, intellectual property, regulatory compliance, environmental impact, and the accuracy of information. By adhering to this Policy, Community Foundation aims to maximize the benefits of AI while minimizing risks and fostering a productive, safe, ethical, compliant, and environmentally conscious environment for all.

For purposes of this Policy, AI tools are software applications, platforms, or online services that use artificial intelligence to autonomously or semi-autonomously create, generate, modify, or analyze content. This includes, but is not limited to, tools that produce or transform text, images, audio, video, code, or other digital content based on user prompts or data inputs (e.g., ChatGPT, Copilot, DALL-E, Midjourney, Gemini, and similar technologies).

SCOPE

This Policy governs the use of AI tools for company-related purposes, whether accessed on company-owned or personal devices, accounts, or networks. The policy applies to all employees, contractors/consultants, temporary staff, volunteers, board members and vendors using AI on behalf of the Community Foundation for Greater Buffalo. Covered Individuals may only use AI tools that have been approved by Community Foundation’s management and/or IT function (or designated technology partner).

Covered Individuals must comply with:

- This AI Acceptable Use Policy
- The Employee Handbook and any applicable codes of conduct
- All applicable laws, regulations, industry standards, and contractual obligations

This policy applies to the use of:

- Generative AI tools

- AI-enabled software platforms
- Automated decision tools
- Embedded AI features in software systems such as AI use within **Microsoft 365 (M365)**, including but not limited to **Microsoft Copilot** experiences in Word, Excel, PowerPoint, Outlook, Teams, OneNote, Chrome and Edge.

1. Acceptable Use:

The following AI tools are approved tools enabled within the Community Foundation environment:

- **Microsoft Copilot** within our M365 environment.
- **Fireflies.ai** (meeting transcription and summarization only)
- **Canva Ai**
- **Zoom Ai Assistant – (Summarization only)**

No other AI tools, websites, browser extensions, plug-ins, or model APIs may be used for organizational work unless **approved in writing** by the Associate Vice President, Administrative Operations (AVPAO) or Chief Financial Officer (CFO).

The Approved AI tools may be used in the following capacity as applicable:

- Copilot
 - Applies to features embedded in M365 apps (e.g., summarize, draft, rewrite, organize).
 - To generate meeting notes or summaries from Teams/Outlook.
 - To create content **drafts** that users will review and correct before external sharing.
 - To draft internal communications (emails, memos, talking points, presentations)
 - To brainstorm ideas, outlines, and alternative ways of expressing concepts
 - To summarize non-confidential documents or publicly available materials
 - To draft or refine non-confidential training materials, knowledge base articles, and customer-facing documentation (subject to review)
 - Improve clarity, grammar, tone, and readability of existing text
 - Conduct high-level preliminary research, with the understanding that facts must be verified through trusted, independent sources
 - For purposes of this policy, internal data may be used only when it is not classified as confidential, highly confidential, donor-protected, financial, health-related, or otherwise restricted. When there is uncertainty about classification, staff must pause and ask before entering content into an AI tool.

- Fireflies.ai
 - For transcription and summaries within organization-approved accounts and for approved meetings with non-sensitive, nonconfidential subject matters or participants.

All AI-generated content must be **reviewed and approved by a human staff member before use or distribution**. AI tools are intended to **assist staff, not replace** professional judgment.

2. Prohibited Actions

Unless explicitly approved by organizational leadership, AI tools may not be used for the following:

- Use unapproved AI tools for company work
- Use personal AI accounts for company work without prior approval
- Enter company credentials (passwords, tokens, API keys, etc.) into any AI tool
- Uploading or attaching files, images, audio, or video to any AI service (including Copilot). Use Copilot's built in summary features only—do not upload attachments to prompts.
- Entering Highly Confidential data (e.g., donor PII, payment data, health information, non-public financials) into prompts.
- Using unapproved AI systems. Unapproved AI tools include, without limitation, public chatbots, browser extensions, plug-ins, model APIs, and consumer AI services such as ChatGPT, Gemini, Claude, and similar tools, unless approved in writing by the AVPAO or CFO.
- Presenting AI generated content as final or authoritative without human validation.
- Customer, client, or prospect lists; pricing models; sales or marketing strategies; bids or proposals; or nonpublic financial reports
- Automated decision-making affecting:
 - program eligibility
 - service delivery decisions
 - employment decisions
- Internal business plans, strategies, research, or analyses labeled as confidential or proprietary
- Create deep-fakes, impersonations, or misleading representations of individuals or organizations
- Circumvent copyright, license terms, or terms of service of AI tools or source content
- Present AI-generated content externally as wholly original human work without meaningful human review and, where appropriate, transparency about AI assistance
- Engage in any activity that would violate existing company policies (e.g., Code of Conduct, anti-harassment policy, social media policy, information security policy)

3. Data Handling & Privacy

Only **Public** or **Internal data may be** used in Copilot prompts; **Confidential data must not** be entered into AI. AI-generated content must be stored and managed in accordance with Community Foundation's information security, communication, and data protection policies.

Where AI tools are approved for organizational use:

- Enterprise or organizational accounts should be used when available
- Privacy settings should be reviewed
- Data-sharing settings should be minimized

Staff should assume that information entered into AI tools may be stored or reviewed by the service provider unless otherwise specified. Use Copilot's built-in **summary and drafting features within Microsoft 365** for content you already have access to. **Do not upload or attach new files, images, audio, or video to prompts.**

4. Accuracy, Attribution, Human Review, and Ethics

AI may be used to support decision-making, but it must not replace human judgment. Final responsibility rests with the Covered Individual and their supervisor, not the AI tool. Decisions affecting people (e.g., hiring, performance evaluations, promotion, termination, compensation, or access to services) must always be made by a human with meaningful review of any AI-assisted materials.

- External-facing materials (e.g., marketing, advertising, sales proposals, client deliverables, investor or shareholder communications, public reports, website content, and social media posts) that rely on AI-generated content must be reviewed and approved by a supervisor or designated reviewer prior to dissemination. Misuse or unethical behavior may result in disciplinary action, up to and including termination of employment
- AI outputs may be incomplete or incorrect; users must **review AI outputs for accuracy, completeness, bias, compliance, and appropriateness before use or sharing**
- Cite sources where appropriate; do not fabricate references
- Disclose AI assistance when required by policy or external agreements
- AI output should be treated as a draft or assistant, not as an authoritative source

5. Ownership of AI-Assisted Work

All AI-assisted work created while performing duties for Community Foundation—including reports, creative works, code, analyses, marketing materials, and other outputs—is the property of Community Foundation. Covered Individuals may not use AI-generated or AI-assisted outputs created for company purposes for personal projects or other commercial endeavors without prior written authorization.

6. Transparency and Disclosure

In some circumstances, it may be appropriate to disclose the use of AI assistance.

Examples may include:

- research reports
- published materials
- donor communications
- policy documents

If staff are unsure whether AI assistance should be disclosed for a report, donor communication, published material, or policy document, they must obtain guidance from leadership before dissemination.

Notification to participants is always required when **Fireflies.ai is active**. For meetings involving minors, board matters, sensitive beneficiary discussions, or confidential donor conversations, Fireflies.ai may not be used unless Operations provides explicit approval in advance.

7. Security & Access Controls

Security and access controls are established at the organization level by the Operations team. The AVPAO (the “Policy Owner”) is responsible for:

- Maintaining the list of approved AI tools
- Defining any conditions or limitations on their use
- Reviewing and approving requests to use additional AI tools

All users must adhere to the following requirements when working with AI tools:

- Use Copilot only with your assigned organizational accounts and approved devices.
- Do not bypass authentication, conditional access, or Data Loss Prevention controls to use AI.
- Follow company cybersecurity practices, including the use of strong passwords, multi-factor authentication where available, and timely software updates
- Understand that many AI tools may log and reuse input data to improve their models, and therefore treat AI inputs as potentially visible to third parties
- Report suspected data exposure or policy violations to Operations immediately

8. Monitoring & Enforcement

Community Foundation reserves the right to monitor and review AI usage for compliance with this Policy. Monitoring may include:

- Periodic audits of AI tool usage within the organization
- Review of AI-generated content used in company work
- Analysis of usage patterns and tools accessed
- Reviewing emerging risks
- Updating policies as technology evolves

This policy should be reviewed at least once annually or when significant technological or regulatory developments occur.

Potential violations of this policy will be addressed under the company's disciplinary procedures and in coordination with HR, the Policy Owner, and/or legal counsel as appropriate. When evaluating potential violations, Community Foundation will consider:

- The severity of the conduct
- The intent of the Covered Individual (e.g., negligent vs. deliberate misuse)
- The actual or potential impact on individuals, data, customers, and the business

Violations of this Policy may result in disciplinary action, up to and including termination of employment or termination of other affiliation with Community Foundation. Misuse of AI tools may also expose both the individual and the company to legal liability.

Any Covered Individual who becomes aware of a suspected or actual violation of this Policy must promptly report it to:

- Their supervisor; and/or
- The Policy Owner (e.g., COO, CIO, IT Director); and/or
- HR or IT, as appropriate

9. Exceptions

Any exceptions must be approved in writing by **AVPAO/CFO**.

10. Legal Obligations

10.1 New York SHIELD Act Compliance

The Community Foundation must implement and maintain reasonable administrative, technical, and physical safeguards for any "private information" of New York residents, as required by the New York SHIELD Act (N.Y. Gen. Bus. Law §§ 899-aa, 899-bb). All AI use must align with these safeguards. Any suspected unauthorized access to private information must be reported immediately.

10.2 Donor Confidentiality Requirements

Donor identifying information, including Form 990 Schedule B contributor information—must not be entered into any AI system. The Foundation will protect donor confidentiality consistent with IRS regulations and internal donor privacy standards. AI tools may not be used to process, analyze, or summarize donor records unless explicitly authorized and restricted to permitted data classifications.

10.3 Meeting Recording & Consent Requirements (Fireflies.ai)

New York is a one-party consent state; however, staff must notify all meeting participants when Fireflies.ai is active. Fireflies.ai must not be used in meetings involving minors, Board Meetings, sensitive beneficiary discussions, or confidential donor conversations unless explicit approval is obtained from Operations

10.4 Vendor Data Protection & Processing (Microsoft & Fireflies)

Microsoft 365 Copilot and Fireflies.ai process information under their respective Data Protection Agreements (“DPA’s”). These services do not use Foundation data to train generalized AI models. All AI use must conform to Microsoft’s and Fireflies’ contractual privacy, security, and data handling commitments.

10.5 Retention, Audit, and eDiscovery Requirements

AI interactions in Microsoft 365—including prompts, responses, and summaries—are subject to Microsoft Purview retention policies, audit logging, and eDiscovery, and will be retained, reviewed, or deleted according to the Foundation’s Records Retention Schedule and legal hold obligations.

10.6 Security Incident & Breach Notification

Any suspected unauthorized disclosure of personal or private information through AI use must be reported immediately to Operations/OITS. The Foundation will comply with all applicable state and federal breach notification requirements, including obligations under the New York SHIELD Act.

10.7 User Responsibility & Liability

Users are responsible for complying with this policy and may be held accountable for intentional or negligent violations, including unauthorized disclosure of donor or private information. The Foundation disclaims responsibility for inaccurate or incomplete AI generated outputs; all users must validate AI assisted content prior to distribution.

10.8 Policy Governance & Review

This policy will be reviewed annually by Operations, MSP for IT, and Legal to ensure compliance with evolving AI, data protection, and nonprofit regulatory requirements.

10.9

Microsoft 365 Copilot Chat operates under Microsoft’s enterprise data protection controls when accessed with a work account. Details are governed by Microsoft’s

official policy:

Microsoft Copilot Chat – Data Protection & Privacy

11. Acknowledgment of Receipt and Review

I, Betsy Constantine (“Covered Individual”), acknowledge that on 7/1/2026 (date), I received and reviewed Community Foundation’s Artificial Intelligence (AI) Acceptable Use Policy. I understand that it is my responsibility to adhere to its guidelines and uphold its principles.

Signature: *Betsy Constantine*

Date: 7/1/2026