

Generic Community Foundation

Acceptable Use Policy

Summary

This Acceptable Use Policy explains how employees and other authorized users must use Generic Community Foundation technology and information systems safely, legally, and professionally. It applies to all devices, accounts, software, networks, cloud services, and data used for Generic Community Foundation business—whether onsite, at home, or while traveling. The goal is to protect donor and constituent trust, keep systems secure, prevent data loss, and maintain compliance with laws and contractual obligations.

Who This Applies To

- All staff (employees full-time and part-time), contractors, interns, temporary staff, volunteers, and any third parties with authorized access (collectively, “Users”).
- All Generic Community Foundation systems and data, whether accessed on organization-owned devices or via approved access methods on managed personal devices.

Core Rules

- Use Generic Community Foundation technology primarily for organization business; limited personal use is allowed only if it is occasional, lawful, does not interfere with work, and does not introduce risk.
- Always protect confidential information. Access, use, and share Generic Community Foundation information only as needed for your job duties and only with authorized individuals.
- Use only approved software, web-based tools, and generative AI solutions for Generic Community Foundation work. If it is not on the approved list (or not explicitly approved), assume it is NOT approved.
- Do not bypass security controls (MFA, endpoint protection, access restrictions). Never share passwords or accounts.
- Report issues immediately (lost devices, phishing, suspected malware, accidental disclosure). Rapid reporting reduces harm.

High-Risk Actions That Are Never Allowed

- Forwarding sensitive Foundation email or files to personal email accounts.
- Storing Foundation files in personal cloud services or unapproved file-sharing tools.
- Entering confidential or non-public Foundation information into unapproved or public generative AI tools.
- Downloading/installing unlicensed or pirated software, or copying/distributing copyrighted materials without authorization.
- Accessing donor, personnel, or financial data without a business need—even if you have permission to access it.
- Using Foundation systems to create, view, transmit, or store discriminatory, harassing, offensive, pornographic, obscene, or illegal material.

Generic Community Foundation

Acceptable Use Policy

Remote Work

- Use secure networks only. Avoid public/unsecured Wi-Fi. If travel requires it, use approved secure access methods.
- Prevent shoulder-surfing. Keep screens and conversations private in shared spaces.
- Do not let family, roommates, or guests use Foundation devices or view confidential information.
- Avoid printing at home. If printing is required, secure documents and shred when no longer needed.

Monitoring and Privacy

Users should have no expectation of privacy when using Foundation systems or accounts. The Foundation may monitor, log, and review system usage (including email, internet access, device activity, and cloud services) consistent with applicable laws and business needs.

Consequences

Violations may result in loss of access, disciplinary action up to and including termination, and potential civil or criminal action where applicable.

Where to Get Help

- When in doubt, ask before acting. Contact the designated technology or operations contact for tool approvals, data handling guidance, or to report incidents. Refer media inquiries to the designated communications lead.

Generic Community Foundation

Acceptable Use Policy

Acceptable Use Policy

1. Purpose

This policy defines acceptable and unacceptable use of Generic Community Foundation technology and information systems to protect confidential information, maintain operational resilience, and meet legal and contractual obligations. Improper use—whether intentional or accidental—can expose Generic Community Foundation to cyberattacks, data loss, service disruption, reputational harm, and legal liability.

2. Scope

This policy applies to all Foundation information systems and technology resources, including computers, phones, tablets, printers, email, messaging and collaboration tools, networks (wired/wireless), internet access, cloud services, applications, storage, and all Foundation data. The policy applies whether systems are owned, leased, or managed by the Foundation and whether access occurs onsite, remotely, or while traveling.

3. Definitions

- “Organization Systems” include all devices, networks, accounts, and cloud services provided or authorized by Generic Community Foundation.
- “Confidential Information” includes donor data, financial data, personnel information, internal strategies, non-public operations, and any information restricted by policy, contract, or law.
- “SaaS” means Software as a Service or web-based applications used to perform work or store/process data.
- “Generative AI” means tools that create content (text, images, code, audio) based on prompts and data inputs.

4. Ownership, Privacy, and Monitoring

- All Foundation Systems, accounts, and Foundation-created information are Foundation property.
- Users have no expectation of privacy in anything created, stored, sent, received, or accessed using Foundation Systems or accounts.
- The Foundation may monitor, log, review, and retrieve system usage (including email, internet, device activity, and cloud services) with or without notice, consistent with applicable law.

5. Acceptable Use

- Foundation technology is provided to support Foundation operations and mission-related work.
- Limited, occasional personal use is permitted only if it is lawful, does not interfere with work, does not consume significant resources, and does not introduce security or reputational risk. The Foundation may restrict personal use at any time.

6. Data Protection and Confidentiality

- Access, use, and share Foundation information only as required for job duties and only with authorized individuals.
- Store Foundation data only in approved Foundation repositories and services; use appropriate permissions and access controls.
- Do not forward sensitive Foundation emails or files to personal email accounts.
- Do not store Foundation confidential data in unapproved cloud services, personal drives, or unapproved devices.
- Report suspected phishing, malware, unauthorized access, accidental disclosures, or lost/stolen devices immediately to the Strategy & Technology Department.

Generic Community Foundation

Acceptable Use Policy

7. Identity, Passwords, and Account Security

- Accounts are individual. Do not share accounts or allow others to use your account, including family or household members.
- Use strong passwords and multi-factor authentication (MFA) as required. Never share passwords or MFA codes.
- Do not approve unexpected MFA prompts. Report suspicious prompts immediately.
- If you lose or replace your phone or authenticator device, contact IT immediately to disable or reconfigure MFA.

8. Devices, Remote Access, and Network Use

- Foundation-issued devices must be secured (password/auto-lock), kept updated, and run approved security software.
- Personal devices may only connect to the guest Wi-Fi network unless explicitly approved and managed by the Foundation.
- Avoid public or unsecured Wi-Fi for Foundation work unless using an approved secure access method.
- Protect devices physically and do not leave them unattended in public places or visible in vehicles.

9. Email, Messaging, and Communications

- Communications must be professional and must not include unlawful harassment, discrimination, threats, or hostile content.
- Do not email or message sensitive personal information (passwords, Social Security numbers, account numbers) unless using an approved secure method.
- Verify external recipients and use approved secure sharing methods for sensitive information.

10. Social Media

- Do not disclose confidential Foundation, donor, employee, or non-public project information.
- Do not post content that could reasonably be viewed as unlawful, defamatory, threatening, harassing, discriminatory, or contributing to a hostile work environment.
- Do not speak on behalf of the Foundation unless authorized. Refer media inquiries to the Marketing Team (or designated communications lead).
- Use good judgment when connecting with or discussing board members, donors, nonprofit partners, or community stakeholders.

11. Software, SaaS Tools, and Generative AI

- Approval required: Users may not download, install, or use software or SaaS tools for Foundation business unless approved by their manager and the Strategy & Technology Department.
- No shadow IT: Do not store or process Foundation data in unapproved services.
- Generative AI: Do not input confidential or non-public Foundation information into unapproved or public AI tools. Approved AI tools must be used in accordance with Foundation guidance.
- Human accountability: Users are responsible for verifying AI outputs for accuracy, appropriateness, bias, and confidentiality before using them in Foundation work.
- Licensing/IP: Do not use copyrighted material unlawfully or violate tool terms. Follow Foundation guidance on AI-generated content and licensing.

Generic Community Foundation

Acceptable Use Policy

- The Foundation may monitor and restrict/block unapproved tools to maintain security and compliance.

12. Unacceptable Use (Prohibited Activities)

- Any illegal activity or violation of local, state, federal, or international law using Foundation resources.
- Installing, distributing, or using pirated or unlicensed software; unauthorized copying or distribution of copyrighted materials.
- Accessing data for non-business purposes, even if you have access.
- Bypassing security controls, scanning/probing networks, or attempting unauthorized access.
- Introducing malware, disabling security tools, or connecting unauthorized devices that create risk.
- Using Foundation systems to procure, transmit, or store discriminatory, harassing, defamatory, offensive, pornographic, obscene, or illegal content.
- Excessive personal use that interferes with work or consumes significant resources.

13. Portable Media (USB/External Storage)

- Portable storage use is permissible for “read only”. Only use secure storage devices.
1. “Write use” onto portable media is only allowed when necessary and explicitly approved by the Strategy & Technology Department and properly secured.
 2. Do not store any confidential information on portable media unless explicitly approved and properly secured.
 - Remove data immediately when no longer needed and store it in approved organization repositories.

14. Training and Compliance

- Annual cybersecurity training is mandatory for continued access to Foundation systems.
- Users must cooperate with incident response, audits, and investigations.

15. Enforcement, Exceptions, and Violations

- Violations may result in loss of access privileges, disciplinary action up to and including termination, and civil or criminal action where applicable.
- Any exception must be documented, approved in writing by Strategy & Technology (and HR/Legal where appropriate), and time-limited with compensating controls.

16. Acknowledgment

All Users must acknowledge they have read, understand, and will comply with this policy as a condition of access to Foundation systems.

Generic Community Foundation

Acceptable Use Policy

Remote Work Addendum

This Remote Work Addendum supplements the Acceptable Use Policy and applies to all Users who access Generic Community Foundation systems outside organization facilities (home, travel, temporary work locations). Remote work is a privilege and may be modified or revoked based on security, performance, or compliance requirements.

1. Remote Work Responsibilities

- Follow all Acceptable Use and Confidentiality requirements.
- Protect Foundation data and systems to the same standard as onsite work.
- Report incidents immediately (lost devices, phishing, suspected malware, accidental disclosure).

2. Approved Access and Shared Environments

- Access Foundation systems only via approved devices and approved secure methods.
- Do not circumvent security controls or allow others to view screens or data.
- In shared/public spaces, prevent shoulder-surfing and ensure confidential conversations cannot be overheard.

3. Home Network and Internet Security

- Use secured, password-protected networks when accessing Foundation systems.
- Avoid public or unsecured Wi-Fi unless using an approved secure access method.
- Maintain home network hygiene: strong Wi-Fi password and updated router firmware.

4. Device and Physical Security

- Keep devices password-protected and auto-locked; do not share devices with household members.
- Keep devices in your possession when traveling; do not leave devices unattended or visible in vehicles.
- Do not check work devices in luggage.

5. Data Handling, Printing, and Disposal

- Store organization data only in approved systems (e.g., approved cloud storage, collaboration, or document-management platforms as configured by Generic Community Foundation).
- Avoid printing at home. If printing is necessary, secure documents and shred or securely destroy them when no longer needed.

6. Travel and International Considerations

- Use heightened caution in travel environments (airports/hotels) due to increased theft and network risks.
- International travel involving access to Foundation systems may require prior approval from Strategy & Technology.

7. Monitoring and Compliance

The Foundation may monitor remote access activity and may restrict or revoke remote access to protect security, compliance, and operations.

Generic Community Foundation Acceptable Use Policy

AI Tools Usage Policy Addendum

This AI Tools Usage Addendum supplements the Acceptable Use Policy and applies to all Users. This document provides guidance on the approved AI tools available to staff, the appropriate use cases for each, applicable usage limits, and the expectations around confidentiality and acceptable use. All staff are expected to review and comply with this policy.

AI tools can significantly enhance productivity when used appropriately. However, it is critical that staff understand which tools are sanctioned, what data can be used within them, and how to use them responsibly.

1. AI Tools Overview

The following example AI tool categories may be approved for use. Each operates at a different level of access, capability, and organizational governance. Replace these examples with the specific tools approved by Generic Community Foundation.

Tool	Access Tier	Primary Access / Notes
General AI Assistant Example	Tier 1 – General	All staff – default example AI tool category for everyday use
Advanced AI Assistant Example	Tier 2 – Advanced	Shared organizational usage pool – for heavier or more complex use cases
Productivity Suite AI Example	Tier 3 – Specialized	Use-case dependent – typically role-based access through an approved productivity suite
Other AI Tools	Requires Approval	Must be approved by Technology AI team prior to use

Generic Community Foundation Acceptable Use Policy

2. AI Tool Details

General AI Assistant Example – Tier 1 (General Use)

The Tier 1 general AI assistant is an example category available to all staff and should be the first tool category reached for day-to-day AI assistance.

Appropriate Use Cases	Privacy & Confidentiality
• Basic drafting of emails, memos, or summaries • Light editing and proofreading • Quick lookups and general Q&A • Brainstorming and idea generation • Light formatting or template completion	The Tier 1 general AI assistant category should be used with a privacy-first approach. Key considerations: • Do not enter personally identifiable information (PII) • Do not input client data, financial records, or confidential internal documents • Suitable for general/public-level information only • Review all AI outputs before use – do not publish unreviewed content

This policy is subject to periodic review and update. Staff will be notified of any material changes.

Last updated: 03-20-2026

Generic Community Foundation

Acceptable Use Policy

Advanced AI Assistant Example – Tier 2 (Advanced Use)

The Tier 2 advanced AI assistant category is available for more intensive AI tasks and may operate on a shared organizational usage pool. Because usage may represent a shared resource, staff should use this category purposefully and for appropriate, higher-complexity tasks.

Appropriate Use Cases	Token Pool – Shared Resource
• Heavy research and in-depth information synthesis • Data analysis and interpretation • Coding, scripting, and technical problem-solving • Complex document drafting and structured writing • Multi-step reasoning and analytical tasks	The Tier 2 advanced AI assistant category may operate on a shared organizational usage budget. Usage is consumed with every interaction. • Use the advanced AI assistant category for tasks where enhanced capabilities are genuinely needed • Use the general AI assistant category for simpler or routine tasks • Avoid excessive re-prompting or repetitive large queries • Misuse may result in restricted access for allowed staff

Productivity Suite AI Example – Tier 3 (Specialized / Role-Dependent)

The Tier 3 productivity suite AI category is integrated into an approved workplace productivity environment and is therefore available only to staff whose roles include access to that suite. Usage is highly dependent on the user's specific role and toolset.

Appropriate Use Cases	Access & Eligibility
• Drafting and summarizing within approved productivity applications • Meeting summaries and action item extraction in approved collaboration platforms • Excel data analysis and formula assistance	• Access is typically limited to senior staff • Available only within the approved productivity suite environment • Availability varies based on your license and role • Contact Technology if you believe you need access

Generic Community Foundation Acceptable Use Policy

- Presentation content generation and enhancement

Generic Community Foundation

Acceptable Use Policy

Other AI Tools – Approval Required

Staff may not use AI tools outside of those listed above unless explicit approval has been granted. This ensures that all AI activity remains within a governed, secure, and compliant environment.

Approval process for new AI tools:

- Submit a request to the designated technology or operations contact via the approved request process.
- Include the tool name, intended use case, data types involved, and business justification
- Await written approval before using any new tool

Questions and Support

If you have questions about this policy, need to request access to a new AI tool, or want to report a concern, please contact the designated technology or operations contact.

Generic Community Foundation

Acceptable Use Policy

Employee Checklist (AUP + Remote Work)

Use this checklist to confirm you are following the Acceptable Use Policy, AI Tools Usage Policy, and Remote Work Addendum. Managers may request this checklist during onboarding, annual policy acknowledgment, or security reviews.

Account & Access Security

- ☐ I use my own Foundation account and do not share credentials or MFA codes.
- ☐ I use MFA correctly and deny/report unexpected MFA prompts.
- ☐ I report lost/stolen phones or authenticator changes immediately.

Devices & Physical Security

- ☐ My device is password-protected and auto-lock is enabled.
- ☐ I lock my screen when stepping away.
- ☐ I keep devices secured during travel and never leave them unattended in public.

Data Handling & Storage

- ☐ I store organization files only in approved repositories (e.g., approved cloud storage or document-management locations).
- ☐ I do not forward sensitive Foundation email to personal accounts.
- ☐ I share files externally only using approved secure methods and only with authorized recipients.
- ☐ I access confidential/donor/personnel/financial data only when I have a business need.

Email, Messaging & Professional Conduct

- ☐ I do not send passwords or sensitive personal identifiers by email or chat.
- ☐ My communications are professional and do not include harassing, discriminatory, or offensive content.
- ☐ I report phishing and suspicious messages immediately.

Remote Work & Networks

- ☐ I use secured networks for Foundation work and avoid public/unsecured Wi-Fi.
- ☐ I prevent others from viewing my screen or overhearing confidential discussions.
- ☐ Household members and guests do not use Foundation devices.
- ☐ I avoid printing at home; if printing is required, I secure and shred documents.

Software, SaaS, and Generative AI

- ☐ I use only approved software and SaaS tools for Foundation work.
- ☐ I do not store or process Foundation data in unapproved cloud services.
- ☐ I do not enter confidential or non-public Foundation information into public/unapproved AI tools.
- ☐ I verify AI outputs for accuracy and confidentiality before using them.

Training & Reporting

- ☐ I complete annual cybersecurity training by the required deadline.

Generic Community Foundation Acceptable Use Policy

☐ I promptly report lost devices, suspected malware, accidental disclosures, and other incidents.

Policy Acknowledgment

I acknowledge that I have received, read, and understand the Acceptable Use Policy, AI Tools Usage Policy, and the Remote Work Addendum. I agree to comply with these requirements as a condition of access to Foundation systems. I understand that violations may result in disciplinary action up to and including termination, and may result in civil or criminal penalties where applicable.

Employee Name: _____

Title/Department: _____

Signature: _____

Date: _____

This policy is subject to periodic review and update. Staff will be notified of any material changes.

Last updated: 03-20-2026