San Francisco Foundation

Artificial Intelligence (AI) Acceptable Use Policy

Updated: 12/8/2025

Introduction

Artificial Intelligence (AI) tools are transforming the way organizations work. They have the potential to automate tasks, improve decision-making, and provide valuable insights into business operations. However, the use of AI Tools also presents new challenges for information security and data protection. This policy is a guide for employees on how to be safe and secure when using AI Tools, especially when it involves the sharing of potentially sensitive company and customer information.

The San Francisco Foundation recognizes that the use of AI Tools can be beneficial to staff but could also pose risks to our data and our clients, including donors and the constituents that we support. Therefore, we are committed to protecting the confidentiality, integrity, and availability of all our data.

Purpose

The purpose of this policy is to establish guidelines for the use of AI Tools at SFF. We encourage the use of AI to increase productivity and innovation, but want to ensure that staff respect privacy, confidentiality, and our data security.

Definitions

- *Artificial Intelligence ("AI")*: An engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.[1] Generative AI, machine learning, deep learning, collaborative filtering, and natural language processing incorporate different aspects of AI.
- *AI Tool:* An application, software, or system that utilizes AI to perform tasks, analyze data, or make or assist in making decisions. This includes AI notetaking tools.
- *Confidential Data*: Nonpublic information about SFF or its business operations, including Personal Data and information defined by SFF policies as "Restricted" or "Confidential".

[1] Cal. Civ. Code § 3110(a).

- *Generative AI*: Artificial intelligence that can generate derived synthetic content, such as text, images, video, and audio, that emulates the structure and characteristics of the artificial intelligence's training data.[2]
- *Intellectual Property ("IP")*: Any creative work or invention protected by law, including but not limited to an organization's logo, trademark, software code, music, video, photo, art, manuscript, or other copyrighted creative work, patented product or design, or trade secret.
- *Personal Data*: Information that could be reasonably linked to an identifiable individual or household, including but not limited to a person's name, street address, email address, phone number, government ID, date of birth, financial data, or health and medical information.
- *Uploading*: Any action that causes information to be transferred to an AI Tool, including transferring files, folders, typing text into a prompt, copying, and pasting, etc.

Policy

This policy applies to all SFF employees and covers any AI technology that staff may interact with.

- **Protection of confidential data:** Employees must not upload or share any data to any unapproved AI Tool (free or paid) without prior approval. Please note that any information provided to a public AI Tool is equivalent to making that information broadly available to the public. See the section below for guidance: ***Data Classification Table.***
- **Compliance with security policies**: Employees must apply the same security best practices when using an AI Tool. This includes using strong passwords, using only software and equipment provided for staff, and following the *SFF IT Acceptable Use policy*.
- **Evaluation and use of AI Tools**: SFF will maintain a list of approved AI Tools. See the section below: **Approved AI Tools**. Prior to using an AI Tool not on the approved list, an employee must receive written consent from the Sr. Director of IT for approval. The requestor should be prepared to discuss the purpose and business justification for using any unapproved AI Tool. Tools that are subsequently approved can be found in the **Approved AI Tools List Change Log** below.
- **Don't trust the output from an AI Tool:** AI-generated content is only suggested data and may be incorrect. AI Tools are generally considered to be "assist" tools and should be double-checked. Be sure to review the output provided by the AI Tool prior to relying on the information.

[2] *Id.* § 3110(c).

- **Stay current with AI IT training:** Take the mandatory AI training. Note that staff must complete these trainings to receive a Microsoft Copilot license:
    - The Fundamentals of Microsoft Copilot: https://sff.cliptraining.com/lesson.cfm?l=42715
    - Microsoft Copilot for Microsoft 365: https://sff.cliptraining.com/course.cfm?c=4893
    - Additionally, staff must complete all Knowbe4 security awareness training.

Policy Compliance

The Sr. Director of IT will verify compliance with this policy through various methods, including business tool reports, internal and external audits, and feedback from employees. Any violation of this policy may result in disciplinary action.

Specific AI Risks

SFF is committed to carefully considering the following AI risks:

- *Accuracy*: AI often learns from and relies on historical data to make decisions or generate content. However, this data may be incomplete, inaccurate or dated and may contain errors that cause the AI algorithms to "hallucinate" (i.e., make up data or the answer) or produce inaccurate information.

- *Privacy*: Many AI tools ingest user prompts into their learning models, so inputting Personal Data could disclose that data to the AI vendor and third-party users without proper notice and consent or in violation of the law.

- *Confidentiality*: If an employee enters Confidential Information (e.g., donor, grantee, or client data, contract terms, marketing plans) as part of an AI prompt, the input could similarly expose the data to the AI vendor, third parties and/or the public, potentially violating contract terms with customers, other third parties, or applicable laws.

- *Intellectual Property Infringement*: AI-generated results that are scraped from databases containing legally protected works may violate intellectual property laws in the U.S. or other countries if used or published without proper authorization. Additionally, employees risk compromising SFF's own intellectual property—or that of its donors, grantees, or clients—if they include proprietary content belonging to SFF or its partners in AI prompts. Furthermore, because AI models can automatically generate images, text, or other content, such output may not be deemed "creative" by courts. As a result, it may lack legal protection and hold limited intellectual property value for SFF. *Fairness and Bias*: AI tools and learning models may incorporate inaccurate, incomplete, outdated, and biased assumptions or data. Therefore, AI tools can produce biased and discriminatory results.

- *Ethics*: AI tools may not filter out violent, extremist, racist, sexist, visually disturbing, or unintended data. Therefore, AI tools may polarize users, undermine respect for self or others, or promote extremist views.

- *Transparency*: Pending regulations and industry guidelines may require companies to explain to the public, regulators, and/or users how their AI technology works and provide information about inputs, computer logic, and testing, including specific decisions and output. However, some developers do not know what data exists in their learning models or how to interpret their AI results. Some developers also may lack documentation about their tools, learning sets, and testing.

- *Security:* AI systems are subject to common cybersecurity attacks such as phishing and ransomware. AI tools are also vulnerable to unique threats such as the "poisoning" of learning models with inaccurate information.

- *Safety*: If not controlled, AI tools also could threaten people's physical health or safety, damage property, and harm the environment.

Approved AI Tools

Any use of AI, via platforms, tools, and software must be consistent with our code of conduct, company policy, and applicable law. Use of AI on company devices must be limited to business purposes. Use of AI tools on personal devices to circumvent company policies or safeguards is strictly prohibited.

The following AI Tools have been vetted by the IT Team and are approved for AI use with *Public Data* and may also be used for *Sensitive Data* under certain circumstances.

See the ***Data Classification Table*** below for data definitions. Staff using these tools can have a reasonable assurance that the information they upload is secure. Additional approved tools and changes can be found in the **Approved AI Tools Change Log** below.

- **Microsoft Copilot** installed on your SFF laptop
- **Microsoft Copilot** on your mobile device
- **Microsoft Copilot** included in the Office 365 product suite via either the online version or in the installed version of the Office 365 apps (Outlook, Teams, Word, etc.)
- **Microsoft Copilot** Recording and Transcription (for Teams meetings)
- **Zoom** using AI Companion (for Zoom meetings)
- **Fathom** Meeting Recording and Transcription (for Teams and Zoom meetings)

AI Notetaking Tools

This following applies to the use of any approved AI notetaking tool.

- **Permissible uses.** Use notetaking tools to record, transcribe, and summarize internal meetings and calls only in accordance with these best practices, this policy, and all other SFF policies and procedures. Notetaking tools should not be used for external meetings and calls. If there is any question whether notetaking tools are permitted for a given use case, please consult the Sr. Director of IT and/or the COO.

- **Get consent from all participants.** All meeting participants should be informed about the use of the recording and/or transcription before it is initiated, through automatic notification and/or instruction from meeting organizers. To that end, enable automatic notification prompts for any time recording or transcription is initiated. This prompt is presented to all meeting participants as soon as recording or transcription starts. Participants joining by phone receive an automated audio notification. If any participant indicates they do not consent, the tool should not be used for that meeting.

- **Limit the use of the "Record" feature.** Consider whether it is essential to record video and audio, or if a transcription and summary are sufficient. Where it is important to record presentations, the "record" feature may be necessary.

- **Do not record or transcribe meetings about sensitive or confidential topics.** Consider which meeting parameters may be too sensitive to record or transcribe. Examples may include sensitive employee conversations. If the recording/transcription has already been enabled, pause the recording/ transcription when discussing confidential details to avoid inadvertent capture.

- **Limit access to recordings, transcripts, and summaries only to those who need it.** Meeting organizers set whether and how meeting participants can use recording features.

- **SFF defaults a retention period to auto-expire all meeting recordings (Teams, Zoom, Fathom) to 30 days**. There are some instances, for example SFF University content, where an exclusion can be made to move recordings from the notetaker tool and store to SharePoint for a longer period. Additional instances of exclusion should be made as a formal request to the Sr. Director of IT for approval. When recordings and transcripts are deleted, the automatically generated summaries tied to those recordings and transcripts are deleted as well. If a longer retention period is necessary for business or legal reasons, care must be taken to ensure the recording is deleted as soon as the reason for retaining it has passed.

- **Review transcripts and summaries for accuracy and confidentiality**. Like all AI tools, notetaking tools may produce inaccurate output. Transcripts and summaries should not be used for official purposes unless and until first subject to human review. Make sure to review transcripts and meeting summaries for accuracy. For example, the notetaking tool may inaccurately identify who is speaking. This is especially true for meetings with many participants (i.e., more than 20). Similarly, meetings and calls that are more than one hour long, with several topics discussed may have inaccurate or less useful meeting summaries. If necessary, meeting organizers and other personnel should be allowed to review and

redact transcripts and meeting summaries to remove confidential and proprietary information.

Prohibited Uses

To ensure the ethical, legal, and best uses of AI within SFF, SFF prohibits the following:

- **Discrimination and Bias:** AI tool shall be used to discriminate or perpetuate unjust and harmful bias against individuals based on their race, color, ethnicity, sex (including pregnancy, childbirth, and related medical conditions; gender identity; intersex status; and sexual orientation), religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law.
- **Unlawful Activity:** No AI system shall be used to engage in fraud, deception, threats, or harassment or to violate any laws, agreements, or industry standards applicable to SFF.
- **Privacy Violations:** Unless approved by the Sr. Director of IT and the COO and used in connection with approved AI tool, SFF employees shall not enter Personal Data into any AI tool or publish such information as part of AI results.
- **Intellectual Property Infringement:** Unless the COO and CFO determines that IP has been properly licensed by SFF or the AI vendor, employees shall not use such IP in connection with any AI tool. This means that, unless approved, employees shall not provide any SFF or other third-party IP to any AI provider as part of a large language model used to train an AI tool, or in any prompt or response to a question from Copilot or another generative AI tool. This also means SFF employees shall not post AI-generated results that include protected IP, unless properly licensed, in any social media posts, marketing, or other commercial or publicly facing materials.
- **Unsafe Activity:** Employees may not use any AI tool that poses a risk to the physical health or safety of individuals, to property or IT systems and networks, or to the environment and natural resources. This means that AI tools must not be used without a defined purpose and human supervision because the use of the AI tools may have unintended consequences.

Data Classification Table

The following table details examples of SFF data and their sensitivity. Any questions regarding this list should be directed to the Sr. Director of IT who may consult with other departments.

Sensitivity	Definitions and Examples
Public Data	Information that the foundation has intentionally placed into the public domain, including: • Published news stories • Public domain information • SFF newsletters • Social media posts • Published annual reports • Audited financial Statements • Published approved grants
Sensitive Data	Confidential Data SFF Intellectual Property Any Personal Data about our applicants, grantees, community members, or SFF personnel: • Any company owned data files that isn't considered *Public Data* • Names, contact, and demographic information • Social security numbers, health information, passport details, etc. • SFF account-related information, such as usernames and passwords • HR data, including personnel files, performance reviews, etc. • Recruiting information, including resume data, interview notes, etc. • SFF Board of Trustees or Employee data (phone numbers, email, physical addresses, etc.)

Approved AI Tools List Change Log

The following AI Tools have been approved for use for specific staff and their department as indicated. The Sr. Director of IT reviewed these tools with the requester for the specific use cases.

AI Tool	Date Approved	Requesting Department	Use Case
CoLoop	June 27, 2024	SLE	The SLE team will summarize grantee data to help answer questions more effectively