INFORMATION TECHNOLOGY / GENERATIVE ARTIFICIAL INTELLIGENCE / RECORDING POLICY TEMPLATE

This template is intended to help organizations develop guidelines for the use of information technology (IT) in the workplace, including generative artificial intelligence (GenAI) tools. It's a starting point with sample language to generate ideas. This template does not cover all the legal, compliance, and organizational requirements that may apply. The right IT Policy for your organization will incorporate input from a wide variety of leaders and experts.

This document does not constitute legal advice. For legal advice regarding your organization's IT policies, you should contact an attorney.

INFORMATION TECHNOLOGY / GENERATIVE ARTIFICIAL INTELLIGENCE POLICY

Last updated on: _____

[Privacy notice: Subject to compliance with applicable laws, we reserve the right to review, monitor, audit, and investigate our workforce's use of information technology on devices we issue or those connected to our network. Please see <<Staff/Workforce/Employee Privacy Notice>> for more information about how we process your information.]

INTRODUCTION

PURPOSE

This IT / GenAI Policy (the "Policy") explains acceptable and prohibited practices related to the use of information technology in our workplace. The purpose of the Policy is to:

- Promote innovation, including through the responsible adoption of emerging technology.
- Safeguard our sensitive, confidential, and proprietary information. Losing control of this information can (1) create legal risks, (2) negatively impact our brand/reputation and relationships, and (3) result in other organizational setbacks.
- Meet our legal and contractual obligations, including privacy and security requirements.
- Reflect our organization's values, including [respect for each other's privacy / autonomy / efficiency]; and
- Avoid unintended harms of modern technology, including:
    - [Amplification of Bias, Discrimination]
    - [Environmental Impact]
    - [Inaccuracy / Hallucinations]
    - [Workplace morale / disengagement]

DEFINITIONS

- **Confidential Information:** Information in any form (oral, written, or electronic) that is (1) identified as *confidential, secret,* or *proprietary*, or (2) revealed in a manner such that a reasonable person would understand such information to be confidential or proprietary in nature. Confidential Information includes all:
    - Information about our strategies, operations, or performance that is not known to the public.
    - Information about past or present Staff that is sensitive in nature, not known to the public, or is otherwise confidential.
    - Information about our partners, stakeholders, and vendors [that is not generally known to the public] [that we have a duty to keep confidential].
    - Personal Information of our Staff, board members, customers, partners, and [other stakeholders].
- **Personal Information**: Any data linked to, or reasonably linkable to an individual, household, or personal device, including any data associated with unique identifiers, such as a device id or randomly assigned user identification number.

- **Recording**: Audio or video data, in any format, with Staff or other individuals' voices or images.
- **Staff**: Our employees, contractors, and other workforce members.
- **Software and Services**: All software, web or cloud-based services, applications, scripts, add-ins, browsers, devices, and browser extensions. Software and Services may require a paid subscription or license or may be provided without cost.
- **Generative AI**: [Software and Services with generative artificial intelligence functionality, including [ChatGPT, Claude, Otter.AI, Gemini, Midjourney…list popular tools used in the workplace or known to be popular by Staff].

SCOPE
This policy applies to our Staff [vendors? anyone connecting to the org's network?].

COMPLIANCE
Violations of this Policy may lead to disciplinary action, including suspension of access to our network, systems, and devices, termination of employment, or legal action.

UPDATES TO THIS POLICY
This Policy shall be reviewed and updated, as needed, biannually. The most recent version of the Policy is always accessible at _____ and may be provided upon request by emailing _____. The history of revisions will be logged at the end of this Policy.

For any questions or clarifications about this Policy, please contact the [PROVIDE CONTACT POINT].

INFORMATION TECHNOLOGY / GENERATIVE ARTIFICIAL INTELLIGENCE POLICY

1. ORG-ISSUED DEVICES AND OTHER IT EQUIPMENT

[Describe policies related to the use of devices and other hardware issued by your organization to Staff.]

Sample:

- Staff must use reasonable and appropriate measures to prevent the loss or theft of, or damage to, org-issued devices.
- Staff must report a lost, stolen, or damaged org-issued device by contacting ____.
- Staff [may/may not] use org-issued devices for incidental and occasional personal use.
- Staff must adhere to <<list and link to other policies>> when using org-issued devices.

2. SOFTWARE AND SERVICES

[Describe the Software and Services Staff can install on org-issued devices and use for work. Consider distinguishing between acceptable uses of Software and Services for (a) core work functions and tasks and (b) use for incidental, low risk tasks.]

Sample text:

Staff may only use IT-approved Software and Services for core work functions and tasks.

- Staff must perform core work-related functions and tasks, and carry out our mission, using the IT-approved Software and Services listed <here> or as we otherwise provide.
- Staff must use IT-approved Software and Services with their work account or credentials.
- Staff may only install IT-approved Software and Services listed <here> or as we otherwise specifically provide.
- Staff may only handle, access, view, collect, record, save, analyze, or otherwise process Confidential Information using IT-approved Software and Services on org-issued devices.
- Staff may only handle, access, view, collect, record, save, analyze, or otherwise process Personal Information using IT-approved Software and Services on org-issued devices, including the Personal Information of past and current members of Staff, consumers, app users, website visitors, and business contacts.

Staff May Use Other Software and Services for incidental, low risk tasks. Staff may use other Software and Services, [including Generative AI services], in accordance with this Policy for **incidental, low risks tasks** provided such use does not involve the access, use, creation, recording, analysis, storage, or processing of Confidential Information or Personal Information. Incidental, low risks tasks are those with minimal impact to our mission, such as:

- Drafting occasional internal-facing materials (e.g., internal email about stress-management or conducting efficient meetings).
- Drafting low risk, low-impact external materials (e.g., a LinkedIn post about a Staff volunteer event, a professional bio for an upcoming conference, a thank-you email for a vendor).
- Generating ideas for non-strategic, non-commercial purposes (e.g., themes for a Staff celebration, icebreakers for a meeting).
- Summarizing or transcribing materials generally available to the public for internal, non-commercial use (e.g., summarizing a speech by a politician or public figure to discuss with team).
- Conducting general research for internal, non-commercial use only.

For the avoidance of doubt, Staff may not:

- Use other Software and Services, including Generative AI services, to perform core work functions.
- Use other Software and Services, including Generative AI services, to process Confidential Information or Personal Information, including the Personal Information of consumers, past and current members of Staff, Board members, website visitors, or app users.
- Upload spreadsheets, documents, recordings, or images to other Software and Services containing Confidential Information or Personal Information.

Personal Use. Incidental and occasional personal use of IT-approved Software and Services [is/is not] permitted.

Requesting IT Approval for new Software and Services. Staff can seek approval for new Software and Services by <describe>. [IT or other org] will assess the Software or Services, engaging other stakeholders, such as Legal and HR, as necessary to complete its review. Software and Services must meet these requirements <<link to separate document describing obligations from applicable data protection laws and regulations, contractual obligations, etc.>>.

3. GENERATIVE ARTIFICIAL INTELLIGENCE SERVICES

[Described policy on use of GenAI.]

Sample text (risk tolerant org):

- Staff may use Generative AI services only in accordance with this Policy.

Acceptable Uses	[List. See incidental, low risks tasks described above.]
Permitted Uses with Approval	[List.]
Prohibited Uses	[List. Possible prohibited uses: • Facial Recognition • Certain IP development • Certain automated decision making.]

Staff [should / should not] use work email accounts when authenticated to Generative AI services.

- Staff must choose inputs to Generative AI Services carefully. Do not input Personal Information or Confidential Information into Generative AI Services, unless [exceptions]. For example, do not share employee Personal Information or our financial information with a Generative AI Service.
- Staff must form prompts for Generative AI Services carefully. Do not ask Generative AI Services for personal, sensitive, or confidential information of other individuals or other organizations. For example, do not ask a Generative AI Services to provide: (1) confidential information of other businesses or organization or (2) Personal Information about a job applicant.

Sample text (risk tolerant org):

- Always review the output of Generative AI Services. Such services may provide outputs, including text and images, which are not accurate or contain biases, or they may produce materials that violate other's intellectual property or other rights. Consider outputs of Generative AI Services drafts or starting points.
- Outputs of Generative AI Services that will be shared outside the organization require extra diligence. Any outputs of such services that will be shared outside of the organization should be proofed, fact-checked, and reviewed to determine if the output may create legal or business risks. For example, AI-generated images should be reviewed for intellectual property risks; AI-generated transcripts should be reviewed for accuracy.
- Consider sustainability when using Generative AI Services. The use of such services can have a significant impact on the environment, given the amount of energy such tools require and the amount of carbon they emit. Put thought into prompts to reduce trial and error; consider alternatives.

4. RECORDINGS

[Describe policy on audio and voice recordings, including through the use of transcription services or with personal devices, for meetings, conversations, board meetings].

Privacy and recording laws apply. Sample text (may not be suitable for all workplaces.

General Recording Policy. [Describe general policy.]

- [Recordings shall only be made in the workplace for the following purposes.....]
- [Recordings may be made strictly in accordance with this Policy. Exercise caution when creating Recordings of meetings, conversations, or other personal interactions between Staff and/or others outside the organization].

Creating Recordings. Recordings may be created in accordance with the rules below, provided such Recordings (1) are created using an IT-approved Software or Services and (2) do not interfere with the Staff's performance.

- Recordings may not be created where and when individuals have a high expectation of privacy, such as in restrooms or a 1:1 meeting about highly personal or sensitive topics.
- *Common areas, larger events where organizer shares information with attendees (e.g., all Staff training event, all-hands meeting)*. Staff may create a Recording in the ordinary course of business in common areas of the workplace or at larger events provided:
    - Recording devices are in plain site or event organizer provides attendees prominent notice that the event will be recorded.
    - Individuals know where they may learn more information about how the Recordings are used and shared; and
    - Such Recordings are only shared for legitimate business needs and lawful purposes.

Privacy and recording laws apply. Sample text (may not be suitable for all workplaces.

- *Meetings, conversations, and other personal interactions*. Staff may create a Recording of a meeting, conversation, and other personal interactions (in-person or virtual) only if:
    - EVERY INDIVIDUAL CONCERNED PROVIDES INFORMED, PRIOR CONSENT to the Recording. Informed, prior consent requires that individuals understand the purpose for the Recording and who will have access to it.
    - The Recording will be used for legitimate business purposes; and
    - The individuals concerned reasonably believe: (1) the Recording will not capture Confidential Information or (2) the benefits of Recording substantially outweigh the risks of unauthorized use and access to Confidential Information.
- *Board Meetings*. The Board may agree to create Recordings of Board Meetings, as needed for legitimate business purposes, in accordance with the Board's bylaws and other governing policies. If the Board creates Recordings, it will do so in accordance with the rules it establishes, providing all Board members have sufficient notice of the rules and when Recordings are created.

Distributing Records.

- Recordings of common areas and large events can only be distributed internally for legitimate business purposes. Approval is required to distribute such Recordings outside the organization.
- Recordings of meetings, conversations, and other personal interactions may be distributed among the individuals concerned and as agreed upon by the individuals.
- Use extra caution when distributing Recordings that contain Confidential Information.

Retaining and Deleting Recordings. Recordings must be deleted within **XX days** unless there is a legitimate business purpose or legal obligation to retain the Recording for a longer period of time. For example, Recordings may be retained for longer when the Recording contains training information or important organizational information.

5. PROHIBITED CONDUCT

[Describe prohibited conduct on network and with org-issued devices].

Sample text:

Staff may not use any of our devices, or the Software or Services we provide, to:

- Create, store, download, distribute, or access:
  - illegal content,
  - pornography or other sexually explicit content,
  - fraudulent, harassing, profane, obscene, intimidating, libelous, slanderous, threatening, abusive, or defamatory materials, or
  - pirated or stolen software, data, or content.
- Access, share, distribute, or send confidential, proprietary, or sensitive information without prior authorization from <_____>. Such information includes, but is not limited to, our copyrighted materials, trade secrets, intellectual property, proprietary financial information, employee information, customer information, or other similar materials that would be considered confidential in nature.
- Scan or scrape information from the web, without authorization.
- Scan or information-gather from our network and systems including the following: port scanning, security scanning, network sniffing, keystroke logging, bit mining and crypto-activities, or other information gathering techniques, when not part of your job function.
- Deliberately propagate, share, or distribute a virus, malware, remote access, reverse proxy, or any other malicious program code.
- Violating any other policies, <e.g., Employee Conduct/Harassment Policy>.

6. NETWORK AND INFORMATION SECURITY

[Describe security policies].

Sample text:

- Security Controls. Staff may not tamper with, bypass, or disable (or attempt to) any security software, controls, or configuration we implement on our network or devices.
- Passwords and Credentials. Staff must use complex passwords and responsible password practices to prevent unauthorized use and access of our network, information, and resources.
  - Passwords should be at least xx characters long and utilize a combination of symbols, numbers, and upper and lowercase letters.
  - Staff may not reuse passwords for unique company related systems and services or use work-related passwords with personal accounts.
  - Passwords and credentials must not be shared with others at any time or left in a place where an unauthorized person might find them. When a need arises to communicate credentials for an approved purpose, doing so must be performed securely.
  - If you believe your password, accounts, or credentials have been compromised, stolen, or discovered by another person, immediately contact _____.

For any questions or clarifications about this Policy, please contact the [PROVIDE CONTACT POINT].

Revision History:

Version Number	*Revision Date*	*Description of Changes*
XX	*July 2025*	

END