City of Cambridge Guidelines on Using Generative Artificial Intelligence (AI)

Information Technology Department (ITD) | November 3, 2025

Purpose of These Guidelines

The purpose of these guidelines is to help City of Cambridge employees use Generative AI tools safely, responsibly, and effectively. The guidelines provide direction on what Generative AI is, best practices on how it should be used responsibly, and how to protect data privacy and security. This is a living document and ITD will regularly update the Guidelines to reflect evolving laws, regulations, lessons learned, and developments in Generative AI technology.

Generative AI is a new type of artificial intelligence technology that can create new content—such as text, images, video, audio, or code—based on prompts or inputs from users. These tools analyze patterns in large datasets to predict and produce relevant outputs. Common examples include ChatGPT, Microsoft Copilot, Google Gemini, and Claude.

While Generative AI has the potential to enhance our work and better serve our community it also poses risks. These include bias, misinformation, hallucinations, factual errors, copyright violations, and inconsistent outputs. These risks are heightened when employees rely on these tools without exercising the necessary human oversight.

Who Should Follow These Guidelines?

All employees, volunteers, contractors, vendors, and anyone representing or working on behalf of the City of Cambridge.

Important Considerations for Generative AI Use

1. Accuracy & Reliability

- A human must always thoroughly review, edit, fact-check, validate and test their AI-generated content before official use. AI tools can make mistakes or provide outdated information. **You are ultimately responsible for any content you use or share.**

2. Data Security & Privacy

Only use City-approved, authorized AI tools for sensitive or confidential data- Personally Identifiable Information (PII) or Protected Health Information (PHI).

- **Personally Identifying Information (PII):** means a person's first name and last name, or first initial and last name, in combination with any one or more of the following data elements that relate to such person:
    - Social Security Number
    - Driver's license number or state issued identification card number; or
    - Financial account number, credit or debit card number with or without any required security code, access code, personal identification number or password, that would permit access to a person's financial account.
    - It does not include information that may be obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.
- If you are unsure whether data is appropriate to input into a City-approved or other Generative AI tool, you can contact ITD Helpdesk or 617-349-4140.
- Always adhere to the City's Written Information Security Policy (WISP) guidelines when handling sensitive data.

3. Bias & Fairness

- AI can unintentionally reflect biases from its training data. Be attentive to potential unfairness or inaccuracies, particularly in content affecting community services, policies, or communications. Regularly review outputs to ensure fairness and accuracy.

4. Transparency & Accountability

- Transparency builds public trust and helps colleagues learn how to use Generative AI responsibly. Expectations on citations may vary by the type of work:

Low-Risk Internal Uses (No Citation Required)

- For routine, internal tasks, you are **not required** to cite or document your use of Generative AI. Examples include:
    i. Drafting internal emails, memos, or communications
    ii. Creating summaries of internal documents
    iii. Writing, editing, or debugging code you can validate

- **Recommended Practice:** To improve team learning and safe use, you are encouraged to share how you used AI—such as prompts or edits made—even when citation is not required.

Medium- to High-Risk Uses (Documentation Required)

- For public-facing or sensitive work, you **must document and disclose** your use of Generative AI. Examples include:
    i. Drafting or translating public-facing content
    ii. Summarizing policy-related or public input data
    iii. Supporting decisions related to services, enforcement, or eligibility
    iv. Contributing to documents that affect regulation, safety, or compliance
- **Requirements:**
    i. Clearly indicate when AI significantly contributed to the content. Include:
        a. A statement that Generative AI was used
        b. The name and version of the tool
        c. A note that the content was reviewed and approved by City staff
    ii. **Sample Credit Line:** "This description was generated/summarized with the assistance of *[Tool Name]* and reviewed by City staff."

Prohibited Practice

- Generative AI should **never be relied upon** to create official City documents or to make decisions that affect residents without expert human review and approval.
    - Users should be aware that AI-generated content (including **prompts** and **outputs**) is subject to public records law and may be considered a public record. Therefore, use of Generative AI must be properly managed and retained by the employee in accordance with all applicable policies and laws of the City and Commonwealth.

Choosing & Using AI Tools

- **City-Approved Tools:** You are encouraged to use City-approved Generative AI tools. Only use City-approved tools for sensitive or confidential data. These tools have been vetted for security, privacy, and appropriate use.

    - Copilot Chat, a Microsoft Generative AI chatbot, is available to City employees. If you log into Microsoft's Copilot with your City account credentials, data you enter or extract from the model will not be used to train the underlying models.

- **Requesting New Tools:** To request an AI tool not currently approved, submit a request through the ITD Helpdesk or appropriate technology procurement channels (like Egov process). All technology acquisitions, including free-to-use software or software-as-a-service tools, must comply with the City's procurement and IT standards and policies.
- **Public Generative AI tools:** These include free, paid, or publicly available chatbots or apps not procured or managed by the City. These tools do not offer adequate privacy or security protections for sensitive or confidential data. Any information shared with them may be used to train the underlying models, creating potential confidentiality risks.
    - While the use of public or consumer Generative AI tools for City business is discouraged, we recognize that such tools may still be used in limited non-sensitive, low-risk circumstances. Any such use must follow the guidance in this document and should never involve confidential, personal, or regulated information.
- **ITD Oversight:** ITD may revoke approval of an AI tool if it is found to pose unacceptable risks.

Your Responsibilities

- **Employees:** Use AI responsibly, ensure outputs are human reviewed, and report any misuse or concerns. **You are ultimately responsible for your work, including content generated by an AI model. You should thoroughly review AI outputs for accuracy and appropriateness of responses.**
- **Managers and Department Heads:** Provide guidance on responsible AI use, ensure your team follows these guidelines, and address any inappropriate use of AI.
- **ITD Staff:** Assist employees with training, using secure and approved AI tools, and oversee tool management.
- **ITD Cybersecurity Team:** Ensure AI use and tools are compliant with City security policies and oversee AI tool evaluations.

Relevant City Policies & Practices

- City of Cambridge Written Information Security Policy (WISP)
- City of Cambridge Computer Use Policy

Contact & Versioning

This is a living document and ITD will regularly update the Guidelines to reflect evolving laws, regulations, lessons learned, and developments in Generative AI technology.

For questions please reach out to the ITD Helpdesk or call 617-349-4140.

This report includes content drafted with support from Microsoft 365 CoPilot. All content was reviewed and finalized by the ITD team.

Glossary

- **Artificial Intelligence (AI):** a broad category of technologies that can perform tasks that typically require human intelligence—such as recognizing patterns, making predictions, or understanding language—by analyzing large amounts of data.
- **Generative AI (Gen AI):** a type of AI that creates new content (such as text, images, code, or audio) based on user prompts, using patterns it has learned from large datasets.
- **Hallucinations:** are false, misleading, or fabricated outputs produced by AI tools that appear credible but are not based on real or accurate information.
- **Personally Identifying Information (PII):** means a person's first name and last name, or first initial and last name, in combination with any one or more of the following data elements that relate to such person:
    - Social Security Number
    - Driver's license number or state issued identification card number; or
    - Financial account number, credit or debit card number with or without any required security code, access code, personal identification number or password, that would permit access to a person's financial account.
    - It does not include information that may be obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.
- **Protected Health Information (PHI):** means any health or medical information that is created or received by an entity and can be linked to a specific person. PHI includes information that relates to:
    - A person's health condition (past, present, or future);
    - The health care or treatment a person has received; or
    - The payment for that care.

  Examples include:
    - Medical record or patient ID numbers
    - Health insurance or subscriber numbers

- Test results, diagnoses, or treatment details
- Prescription information
- Bills or claims that include a person's name or health details
- It does not include information that may be obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.

Quick Guide

Category	Do	Don't
Accuracy & Reliability	Thoroughly review, edit, and fact-check all AI outputs before use.	Share or publish AI-generated content without human review.
Data Security & Privacy	Only use City-approved tools (such as Microsoft Copilot) for sensitive or confidential data- Personally Identifiable Information (PII) or Protected Health Information (PHI)- and comply with the City's Written Information Security Program (WISP).	Enter Personally Identifiable Information or Protected Health Information into non-approved AI tools.
Bias & Fairness	Check outputs for fairness, accuracy, and inclusivity.	Rely on AI outputs that may be unfair or inaccurate.
Transparency & Accountability	Disclose when public facing or sensitive work is AI-generated or AI-assisted to maintain public trust.	Present AI-generated content in public facing or sensitive work as entirely your own without acknowledgment.
Public Records	Save prompts and AI outputs used for City business as public records per WISP.	Delete or fail to retain AI-generated work that qualifies as a public record.
Tool Selection	Employees are encouraged to use City-approved tools or request new ones via the ITD Helpdesk. While the use of non-approved tools is discouraged, we recognize that such tools may still be	Enter Personally Identifiable Information or Protected Health Information into non-approved AI tools.

	used in limited non-sensitive, low-risk circumstances.	
Responsibilities	Employees: Use responsibly & thoroughly review outputs. **You are ultimately responsible for your work**. Managers: Monitor team compliance via regular checks. ITD: Provide oversight & training.	Assume AI tools replace human judgment or responsibility.