Preliminary Use Guidance: Generative Artificial Intelligence

1.0 Overview

As the capabilities of Generative Artificial Intelligence (Generative AI) develop and become more integrated with existing software and systems, agencies may be inclined to explore procuring such tools to use in their business operations, and agency staff may be curious about the ways in which generative AI could impact their work. Utilizing Generative AI Tools could benefit agency operations, for example by automating routine procedures, crafting professional communications, or assisting in learning a new skill. However, this technology is still rapidly changing, and there are meaningful concerns about its reliability and fairness, information privacy and security implications, and how its use may impact public trust.

2.0 Purpose

The Office of Technology and Innovation (OTI) is issuing this preliminary guidance to support agencies in their exploration of Generative AI Tools.

3.0 Authority

OTI is committed to supporting agencies in their exploration of Generative AI. The guidance below lays out key considerations for agencies and their personnel with respect to the use of Generative AI tools and outlines critical policy requirements for agencies. OTI will update this guidance as needed on an ongoing basis, as the technology and considerations for use evolve.

4.0 Terms and Definitions

- **4.1 Generative Artificial Intelligence** ("Generative AI") - Any AI system whose primary function is to generate content, which can take the form of code, text, images, and more.
- **4.2 Generative AI Tools** - The integration of Generative AI models into a variety of software or browser applications, including word processors, email, calendars, and chatbots, which may be run locally or by an application programming interface ("API").
- **4.3 Acceptable Use Policy** ("AUP") - A document that outlines the appropriate use of access to an agency's network, the internet, email or other resources.
- **4.4 AI-Generated Content** - Any content produced by Generative AI.

5.0 Roles & Responsibilities

As with all technology products and tools, individuals should access Generative AI Tools only when such access has been approved by responsible agency personnel, and as authorized by agency-specific and citywide requirements. The relevant personnel and requirements may vary across Generative AI Tools, but will frequently include the following responsible agency personnel:

- **5.1** Agency Chief Contracting Officer (ACCO)
- **5.2** Agency General Counsel
- **5.3** Agency Chief Information Officer (CIO) or Agency Chief Technology Officer (CTO)
- **5.4** Agency Chief Information Security Officer (CISO)
- **5.5** Agency Privacy Officer (APO)

5.6 Agency Algorithmic Tools Liaison[1]
5.7 Various business or operational owners

6.0 Guidance on Using Generative AI Tools for City Agencies

This Guidance builds upon New York City's AI Principles[2] and applies them specifically to Generative AI systems.

6.1 Cybersecurity

Unauthorized or unsupervised use of Generative AI Tools within agency operations may lead to the disclosure of city data in a manner that violates Citywide Cybersecurity Policies and Standards, and may constitute a cybersecurity incident. To enhance the security of Generative AI Tools, agencies should:

- Review the internal agency policies that govern the use of technology and software, including Acceptable Use Policies and Citywide Cybersecurity Policies and Standards before using Generative AI Tools. Conduct comprehensive due diligence when considering vendors for AI capabilities to ensure they meet Citywide Cybersecurity Policies and Standards.
- Consult Agency CISOs prior to considered use of Generative AI Tools.
- Incorporate foundational secure-by-design principles from the outset in the development and deployment of AI systems.
- Immediately report all suspected cybersecurity incidents to the 24/7 Citywide Security Operations Center (SOC).

6.2 Information Privacy

Unauthorized or unsupervised use of Generative AI Tools within agency operations may result in the collection or disclosure of identifying information in a manner that violates the law and citywide privacy policies.

When considering the use of Generative AI Tools, agencies should consider how such use aligns with New York City's privacy principles, which reflect values underlying agency practices and should be honored in all aspects of decision-making and operations.

- APOs should be consulted prior to considered use of Generative AI Tools.
- Agency personnel should review the internal agency policies that govern the handling of identifying information, as well as the New York City Identifying Information Law and Citywide Privacy Policies.

---

[1] Local Law 35 of 2022, Administrative Code of the City of New York, § 3-119.5, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4265421&GUID=FBA29B34-9266-4B52-B438-%20A772D81B1CB5.
[2] Artificial Intelligence: Principles & Definitions.

- Unauthorized agency collection or disclosure of identifying information should be immediately reported to the APO.
- APOs may also reach out to the Office of Information Privacy at OIP@oti.nyc.gov to discuss the application of privacy law and policy to potential agency use cases.

6.3 Trust and Responsibility

Generative AI Tools produce content automatically and without critical reasoning or the ability to fact-check. In general, Generative AI attempts to predict the best response to a prompt based on the materials (text, images, audio and/or video) on which it was trained. If those materials are outdated, incorrect, or biased, the generative AI tool is likely to replicate those traits. Because Generative AI allows the creation of almost endless content with little individual effort, any errors and biases can have an outsized impact. Accordingly, agencies should:

- Ensure any AI-Generated Content is reviewed by personnel before being shared or considered final. If review at the time of generation is not feasible, e.g., in the implementation of a chatbot, procedures should be in place to regularly assess the quality of responses.
- Independently validate AI-Generated Content, e.g., through trusted publications and websites, or with a subject matter expert.
- Verify that any citations produced by the tool are valid and correctly used.
- Consider the potential for representational harms due to inherent biases in AI-Generated Content taking care to ensure, for example, that people and residences depicted in AI-Generated Content accurately reflect the diverse communities residing within the city.
- Consider the resources needed to operate and maintain a Generative AI Tool that will be able to keep up with the rapid pace of innovation. Such needs include maintaining consistency with the city's AI Principles, active product management, technical reviews and assessments, upgrades, funding, and compliance with applicable laws.

6.4 Transparency

In order to support critical engagement by end users and maintain public trust in city government, it is best practice to proactively disclose the use of Generative AI in all contexts. Agencies should therefore:

- Always label AI-Generated Content as such, even if it has been edited by personnel. Examples of labeling may include a header or footnote in a document containing AI-Generated Content, or a standing notice on a webpage through which a Generative AI Tool is accessed.
- Consider using "watermarking" capabilities offered by Generative AI Tools, when available, to track the use of AI-Generated Content, but be aware of the currently assessed limitations. AI watermarks manipulate AI-Generated Content so that an algorithm can recognize the output as AI-generated. This manipulation is meant to provide a subtle signature that content was created with a Generative AI Tool. However, current AI watermarking

technologies can introduce significant distortions in AI Generated Content, and are in general not stable within downstream manipulations such as image cropping or text summarization. As the technology matures, OTI will continue to look for enterprise solutions that validate authorship securely within a text, image, audio, or video.

- Understand when uses of Generative AI may count as an algorithmic tool under Local Law 35 of 2022[3] and therefore must be included in annual compliance reporting. Consult with your agency's Algorithmic Tools Liaison for more information.
- Remember that interactions with Generative AI Tools, including prompts and other inputs, may be covered by other areas of law, including New York State Freedom of Information Law and New York City Open Data Law.

7.0 Ownership

This guidance is provided by OTI's Strategic Initiatives Division. For questions related to this document, please reach out to your Agency Relations Manager.

8.0 Related Laws & Policies, Requirements, and Processes

8.1 Laws

- New York State Freedom of Information Law
- New York City Open Data Law
- New York City Identifying Information Law
- New York City Local Law 35 of 2022

8.2 Citywide Policies

- Artificial Intelligence: Principles & Definitions
- Citywide Privacy Protection Policies and Protocols of the Chief Privacy Officer
- Citywide Cybersecurity Policies and Standards

8.3 Processes

- Cloud Review
- Procurement
- Software Security Assurance Process (SSAP)

8.4 Agency-Specific Policies

- Various internal business processes and use policies
- Agency cybersecurity policies
- Agency privacy policies
- Agency Acceptable Use Policies

[3] Administrative Code of the City of New York, § 3-119.5, supra note 1.

9.0 History and Ownership

Version	Change Description	Author(s)	Date
1.0	Inaugural version	Alex Foard, Jiahao Chen and Renata Gerecke, Strategic Initiatives Division	03/04/2024