City Policy	Subject: Acceptable Use of Artificial Intelligence by Employees	Policy No. CITY-IT- 304
Effective Date: 11/01/2026	Issued By: City Manager	

Artificial Intelligence (AI) Acceptable Use (Employees)

1. Purpose

The City recognizes that artificial intelligence ("AI") tools (including "generative AI") may improve efficiency, productivity, and service delivery by assisting with routine drafting, training materials, data analysis, and other administrative tasks. At the same time, AI tools may generate inaccurate or biased information, expose confidential information or protected data, undermine transparency, or create legal, operational, cybersecurity, employment, or public trust risks if used without appropriate human review and governance.

For the purposes of this Policy, AI is defined as machine-based systems that can, for a given set of human-defined objectives, make predictions, recommendations, decisions, or take actions that influence real or virtual environments.

This Policy establishes clear requirements governing the responsible, lawful, and transparent use of AI in connection with City business.

2. Scope

This policy applies to all City employees, contractors and users of the City IT equipment and governs any use of AI tools in connection with City business, whether:

- Accessed on City-owned devices or systems or personal devices used for City work.
- Accessed through third-party applications or web-based tools.
- Embedded within other software platforms used by the City.

This Policy supplements, and does not replace, other applicable City policies, including those addressing acceptable use of technology, confidentiality, public records, records retention, cybersecurity, employment practices, and workplace conduct.

3. Guiding Principles

All City use of AI shall be governed by the following principles:

- **Human accountability:** Employees remain responsible for all work product and decisions. AI outputs must be reviewed and verified by employee before use.
- **Privacy and confidentiality:** The City's confidential information and sensitive data must be protected and not exposed to unauthorized systems or vendors.
- **Security:** AI use must align with City cybersecurity policies, standards and risk-management practices.
- **Fairness and non-discrimination:** AI must not be used in ways that unlawfully discriminate against or produce unjustified disparate impact in employment, services or procurement.
- **Transparency and public trust:** The City must be able to explain, defend, and document official actions, including actions informed by AI.

4. Permitted Usage

When using City-approved AI tools and subject to all other City policies, employees may use AI to assist with:

- Drafting or improving non-confidential documents or communications (e.g., general communications, formatting assistance, brainstorming).
- Summarizing City-owned, non-confidential materials, consistent with records-retention obligations.
- Creating training outlines or administrative checklists that do not include confidential or protected information.
- Usages embedded within city-provided AI tools or resources.
- Basic research support as a starting point, with independent verification.

All AI-generated output must be reviewed, edited, and validated by the employee before use. Employees must not rely on AI outputs as authoritative or final without independently informed judgment.

5. High Sensitivity Data

High Sensitivity Data consists of information that is individually identifiable, highly sensitive, or confidential, where unauthorized disclosure could cause significant harm. Such data must be handled carefully with AI tools because improper use can result in serious legal and security risks.

Examples of High Sensitivity Data include:

- Attorney/Client privileged information
- Login credentials for technology systems
- Protected health information (HIPAA)
- Social Security numbers
- Credit card numbers (PCI)
- Other identifiable health/medical information
- Other financial account numbers (such as bank account numbers)
- LEADS/CJIS data
- Confidential Law Enforcement Investigatory Records

6. Prohibited Usage

Employees may NOT:

a. Input or upload High Sensitivity Data into AI tools not provided or approved by the City for such reason.

b. Use AI to make or substantially influence employment decisions, including hiring, promotion, discipline, discharge, evaluation, or compensation without an established process for validation and human oversight.

c. Use AI tools to conduct covert monitoring or surveillance of employees or members of the public beyond what is necessary for legitimate City purposes.

d. Use AI to create false, misleading, or deceptive records or content**,** including altered or fabricated documents, audio, video, or images purporting to represent City actions or officials.

e. Use AI to generate deepfakes or deceptive content (images, audio, video) involving City officials, employees, or residents, or to mislead or deceive the public.

f. Use AI as a substitute for legal advice or to assess liability.

g. Use recording/transcription/note-taking apps not provided by the City (including AI-enabled apps) to record meetings, interviews, or conversations involving City business unless authorized and consistent with applicable law and City policy.

h. Use AI in a manner that violates law, City policy, or standards of professional conduct, including discriminatory, offensive, or harassing uses.

7. AI-Generated Content and Images

Departments are responsible for making sure AI-generated content follows copyright laws, licensing requirements, public records laws, and other legal and transparency requirements. Because current AI image tools may create copyright or intellectual property concerns, employees must use these tools carefully and openly.

Image Use Guidelines

a. Employees **may use** approved AI tools to create graphics, presentations, diagrams, charts, training materials, and other visual content that supports their work.

b. Employees **must not** use AI to create or modify copyrighted images, including the City's logo, branding, or other protected materials.

c. Employees **must not** create AI-generated images, as a substitute for authentic photographs or documentary images, that could reasonably lead the public to believe they show a real person, object, event, place, condition, or occurrence when they do not.

d. AI-generated images of residents, employees, elected officials, public safety personnel, or other identifiable individuals are **not allowed** unless approved by the City Manager or designee.

e. Employees **must clearly identify** when AI was used to create content.

f. Employees **must review** all AI-generated work for accuracy, quality, and appropriateness before sharing or publishing it.

8. Data Handling, Confidentiality, and Privacy

Employees must assume that AI prompts and outputs may be retained by vendors and may be subject to audit, discovery, or disclosure.

9. Public Records, Retention, and Transparency

AI-related materials, including prompts, outputs, drafts, emails, logs, reports, and decisions influenced by AI, may constitute public records under Ohio Revised Code Section 149.43 if created or used in the transaction of City business, unless a statutory exception applies.

AI-related records must be retained in accordance with applicable records-retention schedules. Employees shall not delete, conceal, or alter AI-related records to circumvent retention obligations or public-records requirements, consistent with Ohio Revised Code Section 149.351.

10. Cybersecurity and Incident Response

AI tools must align with the City's cybersecurity program and security controls. Employees shall not enter City credentials into services not provided by the City, bypass security safeguards, or reuse passwords.

Any suspected AI-related data exposure or misuse must be reported promptly to IT and the employee's supervisor in accordance with City incident-response procedures.

11. Training, Governance, and Support

The City may provide training on responsible AI use, confidentiality, cybersecurity, and public-records obligations. Departments with higher-risk data or use cases may receive role-specific guidance. IT may not be able to provide support with AI tools that are not provided by the City.

12. Oversight and Review

The City reserves the right to monitor, audit, restrict, suspend, or discontinue the use of any AI tool or use case at any time to ensure compliance with law, City policy, security requirements, and public-trust obligations. The City may review AI usage, outputs, and associated practices to assess risk, effectiveness, and compliance.

This Policy may be reviewed periodically and updated as necessary to reflect changes in technology, law, regulatory guidance, and City operations. Continued use of AI tools is subject to ongoing compliance with this Policy and any updated guidance issued by the City.

13. Violations and Enforcement

Violations of this policy may result in corrective action, up to and including discipline, termination, and/or referral for investigation, depending on severity. Misuses involving confidential information, resident data, deception, or security violations may also lead to legal action.