

RECORD OF RESOLUTIONS

Resolution No. 2026-15R
Passed October 20 20 26

A RESOLUTION ADOPTING AN ACCEPTABLE USE OF ARTIFICIAL INTELLIGENCE POLICY OF THE CITY OF PICKERINGTON

WHEREAS, the City of Pickerington recognizes both the benefits and risks associated with fast-changing and ever-evolving artificial intelligence (AI) tools; and

WHEREAS, the City is committed to leveraging technology and available tools to enhance its services to residents while at the same time maintaining oversight and human responsibility for the outputs of such tools; and

WHEREAS, in pursuit of that goal the City has drafted an Acceptable Use of Artificial Intelligence Policy that shall be implemented and enforced for all non-police City employees; and

WHEREAS, the Police Department shall produce its own policy for AI use in light of the sensitive nature of its work.

NOW, THEREFORE, BE IT RESOLVED BY THE COUNCIL OF THE CITY OF PICKERINGTON, FAIRFIELD-FRANKLIN COUNTIES, OHIO, A MAJORITY OF ITS MEMBERS CONCURRING:

SECTION 1. City Council hereby adopts the Artificial Intelligence Acceptable Use Policy attached hereto and incorporated herein as Exhibit A.

SECTION 2. That this resolution shall take effect and be in force from and after the earliest period allowed by law.

APPROVED BY: [Signature] Mayor
Lee A. Gray, Mayor

DATE OF APPROVAL: October 20, 2026

EFFECTOVE DATE: October 20, 2026

ATTEST: [Signature] (for H. Moore)
Heather Moore, City Clerk

SPONSOR: SERVICE COMMITTEE

APPROVED AS TO FORM AND LEGALITY OF PURPOSE: [Signature] on behalf of
Philip K. Hartmann, Law Director

CITY OF PICKERINGTON

Artificial Intelligence (AI) Acceptable Use Policy

Effective Date: [DATE] | Last Reviewed: [DATE]

1. Purpose

The City recognizes artificial intelligence ("AI") tools, including generative AI and AI-powered assistants embedded in productivity software, may improve efficiency, productivity, and service delivery. The City encourages employees to explore and adopt AI tools responsibly to enhance their job functions and improve the services the City delivers to residents. AI tools may assist with routine drafting, training materials, data analysis, research, financial reconciliation, and other administrative tasks.

At the same time, AI tools may generate inaccurate, biased, or fabricated 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 purposes of this Policy, AI is defined as machine-based systems that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions, or take actions that influence real or virtual environments. This definition encompasses:

- Generative AI tools (e.g., tools that produce text, images, audio, video, code, or other content in response to prompts);
- Large Language Models ("LLMs"), which are AI systems trained on large volumes of text data and capable of generating human-like text, summarizing documents, answering questions, writing code, and performing other language-based tasks;
- AI-powered features embedded within licensed City software platforms (including, but not limited to, Microsoft 365 Copilot and similar productivity-suite assistants); and
- AI agents and automated workflows, meaning AI systems or pipelines that can take multi-step actions, interact with external services, generate and send communications, or execute tasks with limited human intervention at each step.

This Policy establishes clear requirements governing the responsible, lawful, and transparent use of AI in connection with City business. 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. It is intended to provide clear guardrails, not to discourage employees from using AI to do their jobs better.

2. Scope

This Policy applies to all non-Police Department City employees and City contractors acting on behalf of the City, or directly employed by the City, 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 (including Microsoft 365 Copilot and similar integrated AI assistants); or

- Deployed as part of automated workflows, AI agents, or pipelines that act on behalf of the City or its employees.

Due to the nature of work and rapidly expanding and evolving procedures and tools available, the Pickerington Police Department shall develop and implement its own policy for the acceptable use of Artificial Intelligence and shall not be bound by the terms of this Policy.

3. Guiding Principles

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

- **Human Accountability and Oversight.**
 - Employees remain personally responsible for all work products and decisions, including those informed or assisted by AI.
 - AI outputs must be reviewed, verified, and edited by the responsible employee before use or distribution.
 - No AI output, including outputs from City-approved tools such as Microsoft 365 Copilot may be submitted, published, or acted upon as authoritative without independent human judgment.
 - Automated AI actions (*e.g.*, agents, workflows) that affect City operations or external parties require prior authorization from the City's Compliance Officer and defined human review checkpoints.
- **Privacy and Confidentiality.**
 - The City's confidential information and sensitive data, whether city, resident, or other, must be protected and may not be entered into unauthorized AI systems or vendor platforms.
 - Employees must understand data entered into AI tools may be retained, processed, or used to improve vendor models unless the City's contractual terms expressly prohibit such retention.
 - AI tools that process City data must be evaluated for data-handling practices prior to deployment.
- **Security.**
 - AI tool use must align with the City's cybersecurity standards, risk-management practices, and approved technology environments.
 - Employees must not enter credentials, passwords, authentication tokens, or sensitive system configuration details into any AI tool not provided or expressly approved by the City.
 - AI tools must not be used to bypass, circumvent, or weaken City security controls, access controls, or data-handling requirements.
 - Departments must report suspected AI-related security incidents promptly in accordance with Section 9 of this Policy.
 - The City IT Department and/or designated IT consultant will maintain a list of approved AI tools and platforms. Use of unapproved AI tools in City systems may constitute a cybersecurity incident.

- AI agents and automated workflows must be reviewed and authorized for use by the IT department and/or designated IT consultant before deployment to ensure they do not introduce vulnerabilities, unauthorized data flows, or unintended access.
- **Fairness and Non-Discrimination.**
 - AI must not be used in ways that unlawfully discriminate or produce unjustified disparate impact in employment decisions, service delivery, or public-facing applications.
 - AI outputs used in high-stakes decisions must be reviewed for bias prior to use.
- **Transparency and Public Trust.**
 - The City must be able to explain, defend, and document all official actions, including actions informed or assisted by AI.
 - Employees must not use AI to obscure the basis for a decision or to create the appearance that a decision was made by a human when AI played a substantial role.
 - Significant AI-assisted recommendations or outputs that influence official decisions should be documented as such in the relevant record.
- **Responsible Use of Embedded and Integrated AI.**
 - City-licensed tools, including Microsoft 365 Copilot, may incorporate AI features that are active by default. Employees must apply the same standards of care, accuracy, and data handling to these embedded AI features as to any standalone AI tool.
 - The presence of AI features within City-approved software does not constitute blanket authorization to use those features for all purposes. Use remains subject to this Policy.
- **Encouragement of Responsible Innovation.**
 - The City recognizes AI tools are rapidly evolving and that responsible experimentation can yield meaningful improvements in City operations and resident services.
 - Employees are encouraged to identify AI use cases that could enhance their job functions and to bring those ideas to their department heads for evaluation.
 - Department heads are responsible for evaluating AI use cases within their departments, consulting with IT as needed, and approving or directing employees on appropriate use within the boundaries of this Policy.
 - This Policy is intended to enable, not impede, thoughtful use of AI by City employees.

4. Permitted Usage

When using City-provided or City-approved AI tools, and subject to all other requirements of this Policy, employees may use AI to assist with the following, provided the activity involves only non-High-Sensitivity Data (see Section 5) unless the specific tool has been approved for such data:

4.1 Document Drafting and Editing

- Drafting, improving, or summarizing non-confidential documents, correspondence, meeting agendas, and communications.
- Formatting assistance, grammar review, and style editing for non-confidential materials.
- Creating templates or standardized language for routine administrative documents.

All AI-drafted documents must be reviewed, substantially edited where appropriate, and validated by the responsible employee before distribution or filing.

4.2 Research and Information Gathering

- Using AI as a starting point for research on non-confidential topics, with all factual claims independently verified before reliance.
- Summarizing publicly available materials or City-owned, non-confidential documents, consistent with records-retention obligations.

Employees must not treat AI-generated summaries or research as authoritative. AI tools may generate plausible but inaccurate or fabricated content (commonly called "hallucinations"). Independent verification is required.

4.3 Training and Administrative Support

- Creating training outlines, learning materials, FAQs, or administrative checklists that do not include confidential or protected information.
- Generating meeting notes or summaries using City-approved transcription tools, subject to applicable recording and consent requirements.

4.4 Data Analysis and Reporting

- Performing analysis on non-confidential City datasets to identify trends, generate visualizations, or support reporting, subject to data-governance requirements.
- Using AI features within approved City platforms (e.g., Microsoft 365 Copilot) to analyze and organize documents, spreadsheets, or communications that do not contain High Sensitivity Data.

4.5 Financial Reconciliation and Analysis

Employees in finance and accounting roles may use AI-powered features within City-approved financial management systems and enterprise platforms to assist with:

- Bank statement reconciliation, transaction matching, and identification of discrepancies;
- Analysis of financial data, expenditure trends, and budget reporting;
- Generation of draft financial summaries, reports, or variance analyses; and
- Routine accounts payable and accounts receivable processing support.

Such use is permitted provided it occurs within City-approved financial systems that have been evaluated by IT for appropriate data security and access controls. Employees must not export or copy financial account data, bank statement details, or transaction records into standalone or third-party AI tools not approved for that data category (see Section 5 and Section 6.1). All AI-assisted financial outputs must be reviewed and validated by the responsible employee before use in official records, reports, or submissions.

4.6 Code and Workflow Assistance

- Using AI to assist with writing, reviewing, or debugging code for non-sensitive City systems, subject to IT review prior to deployment.
- Developing internal process-automation workflows using City-approved platforms, subject to review requirements in Section 6.

In all cases, the responsible employee must review, validate, and take accountability for the final work product.

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 with

particular care in connection with AI tools, because improper use can result in serious legal, security, and reputational risks.

Examples of High Sensitivity Data include:

- Attorney-client privileged communications and work product
- Login credentials, passwords, and authentication tokens for City technology systems
- Protected health information (PHI) subject to HIPAA
- Social Security numbers and government-issued identification numbers
- Payment card numbers and data subject to PCI (Payment Card Industry) DSS (Data Security Standard).
- Other individually identifiable health or medical information
- Financial account numbers (e.g., bank account numbers, routing number
- Personally identifiable information (PII) of residents, employees, or third parties beyond what is necessary for the task
- Confidential personnel records, including disciplinary, medical, and compensation information

The inclusion of financial account numbers and bank statement data in this category does not prohibit their use within City-approved financial management systems and enterprise platforms that have been specifically evaluated and approved by IT for that purpose (see Section 4.5). The prohibition in Section 6.1 applies to inputting such data into AI tools outside those approved environments.

Employees must not input High Sensitivity Data into any AI tool not expressly approved by the City for that data category. Use of City-approved tools such as Microsoft 365 Copilot for tasks involving High Sensitivity Data is subject to IT guidance on approved configurations and data-handling requirements for that platform.

6. Prohibited Usage

The following uses of AI are prohibited for all City employees:

6.1 High Sensitivity Data in Unapproved Tools

Employees shall not input, upload, or paste High Sensitivity Data (as defined in Section 5) into any AI tool not provided or expressly approved by the City for that data category and shall not be uploaded into any AI platforms outside of the course and scope of employment.

6.2 Employment Decisions Without Human Oversight

Employees may not use AI to make or substantially influence employment decisions including hiring, promotion, discipline, discharge, performance evaluation, or compensation without an established, documented process for human validation and oversight. AI tools must not replace manager or supervisor judgment in these processes.

6.3 Automated Communications

Employees may not configure or use AI agents, workflows, or tools to automatically generate and send emails, letters, text messages, social media posts, or other external communications on behalf of the City without explicit prior authorization from a supervisor and department head. All outbound City communications must reflect a human review and approval step before transmission. This prohibition applies regardless of the platform, including automation features within Microsoft 365 and any other City-approved tool.

6.4 Unauthorized AI Agents and Automated Workflows

Employees may not deploy AI agents or automated multi-step workflows that interact with City systems, external services, or the public without prior review and written approval from IT and/or a designated IT consultant and the employee's department head. Any approved AI agent must include defined human oversight checkpoints, logging, and the ability to be halted immediately if it operates outside intended parameters. See section 3 above.

6.5 Covert Monitoring and Surveillance

Employees may not use AI tools to conduct covert monitoring or surveillance of employees or members of the public beyond what is expressly authorized by applicable law and City policy.

6.6 Deepfakes, Synthetic Media, and Deceptive Content

The creation or use of AI-generated synthetic media involving City employees, elected officials, appointed officials, or residents is strictly prohibited. Specifically, employees may not:

- Create, commission, or distribute AI-generated images, photographs, video, audio, or any other synthetic likeness depicting any City employee, elected official, appointed official, or resident, whether for internal or external purposes;
- Use AI tools to alter, manipulate, or digitally modify authentic photographs, video recordings, or audio recordings of any City employee, elected official, appointed official, or resident in a way that misrepresents their appearance, actions, or statements;
- Create AI-generated deepfakes or fabricated media purporting to show anyone making statements, taking actions, or appearing in situations that did not occur; or
- Use AI to generate or distribute content designed to mislead, deceive, or impersonate City employees, elected officials, appointed officials, or residents, or the City itself.

This prohibition applies regardless of whether the content is intended as satire, parody, internal use, or any other framing.

6.7 False, Misleading, or Deceptive Records

Employees may not use AI to create false, misleading, or deceptive records or content, including altered or fabricated documents, official reports, transcripts, or public communications purporting to represent City actions or positions.

6.8 Substitute for Legal Advice

Employees may not use AI as a substitute for legal advice or to assess City legal liability. Questions requiring legal judgment must be referred to the City Law Department.

6.9 Unauthorized Recording

Employees may not use recording, transcription, or AI-enabled note-taking applications not provided or approved by the City to record meetings, interviews, or conversations involving City business, unless authorized and consistent with applicable law and City policy.

6.10 Violations of Law or Policy

Employees may not use AI in any manner that violates applicable law, City policy, or professional standards of conduct, including uses that are discriminatory, harassing, offensive, or otherwise contrary to City values.

7. Microsoft 365 Copilot, LLMs, and Embedded AI Tools

Large Language Models (LLMs) are AI systems trained on large volumes of text and capable of generating human-like text, answering questions, summarizing content, and assisting with a wide range of language tasks. LLMs power many AI tools, including standalone tools (such as ChatGPT, Claude, Gemini, and others) and embedded features within platforms the City already licenses.

Microsoft 365 Copilot is an AI assistant embedded within the City's Microsoft 365 environment (including Outlook, Word, Excel, PowerPoint, Teams, and related applications). Because Copilot operates within the City's licensed Microsoft 365 tenant, it may have access to City data across those applications by design.

Employees using Microsoft 365 Copilot or other LLM-based tools within City platforms must observe the following requirements:

- Copilot and similar embedded AI tools are subject to this Policy in full, including all prohibitions on use of High Sensitivity Data, automated communications, and prohibited content.
- Employees should not assume that City data processed by Copilot is automatically protected from external use or retention. Employees must follow IT guidance regarding approved Copilot configurations and data-handling settings.
- Copilot's drafting, summarization, and analysis features must be reviewed by the responsible employee before the output is used, shared, or relied upon. AI-generated outputs are not authoritative.
- Employees must not use Copilot or Microsoft 365 automation features (including Power Automate or similar tools) to send automated external communications without the explicit prior authorization required in Section 6.3.
- Embedded AI features that the City has not specifically evaluated or approved for a particular use case should be treated with the same caution as any unapproved AI tool for that use case.

Employees should contact IT with questions about whether a particular use of an embedded AI feature is authorized.

8. AI Agents and Automated Workflows

AI agents are AI systems or pipelines that can take sequences of actions, interact with external services, make decisions across multiple steps, and execute tasks with limited human intervention at each step. Examples include AI tools configured to automatically draft and send communications, retrieve and process data from multiple systems, create or modify files or records, or interact with City residents or external parties on behalf of employees.

AI agents present heightened risks because errors or misconfigurations can propagate automatically and at scale. The following requirements apply to all AI agents and automated AI workflows used in connection with City business:

- **Prior Approval Required:** No AI agent or automated AI workflow may be deployed for City use without prior written approval from the employee's department head and the City IT Department.
- **Human Oversight Checkpoints:** All approved AI agents must include defined points at which a human employee reviews and approves actions before they are taken, particularly for any actions affecting external parties, residents, or official City records.
- **No Automated External Communications:** AI agents may not automatically send emails, letters, messages, or other communications to parties outside the City without human review and approval of each communication prior to transmission, consistent with Section 6.3.

- **Logging and Auditability:** AI agents must maintain logs of actions taken, sufficient to allow review, audit, and reconstruction of the agent's activity. Logs are subject to public-records requirements.
- **Kill Switch / Halt Capability:** All AI agents must be configurable to halt immediately if they operate outside intended parameters. The responsible department must maintain the ability to disable the agent without IT assistance in urgent situations.
- **Scope Limitation:** AI agents must be configured with the minimum access to City systems and data necessary to perform their authorized function. Agents must not be granted broad or administrative-level access to City systems.
- **Periodic Review:** Approved AI agents must be reviewed at least annually by the responsible department and IT to assess continued appropriateness, security, and compliance with this Policy.

9. 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, public records request, or disclosure. Employees should craft AI prompts accordingly and must not include information in prompts that they would not be comfortable having disclosed.

Before using any AI tool with City data, employees should seek guidance from IT and/or the City's designated IT consultant regarding whether the tool's data-handling practices are consistent with the City's confidentiality, privacy, and security obligations.

10. Public Records, Retention, and Transparency

AI-related materials including prompts, outputs, drafts, emails, logs, reports, and records of decisions informed 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.

Logs generated by AI agents and automated workflows are subject to the same retention requirements as other City records.

11. Cybersecurity and Incident Response

AI tool use must align with the City's cybersecurity program and all applicable security controls. The following requirements apply:

- **Approved Tools Only:** Employees must use only AI tools approved by IT for City business. The IT Department will maintain and publish a list of approved AI tools. Using unapproved tools in connection with City data or systems may constitute a cybersecurity incident.
- **No City Credentials in Unapproved Services:** Employees must not enter City credentials, passwords, authentication tokens, or other access information into AI tools or platforms not provided or approved by the City.
- **No Password Reuse:** Employees must not reuse City account passwords for AI tool accounts or services.

- **No Circumvention of Security Controls:** AI tools must not be used to bypass, weaken, or circumvent City security controls, network monitoring, access management, or data-loss prevention measures.
- **Data Minimization:** Employees should avoid including more City data in AI prompts than is necessary to accomplish the specific task.
- **Incident Reporting:** Any suspected AI-related data exposure, unauthorized access, system compromise, or misuse must be reported promptly to the City IT Department and the employee's supervisor in accordance with City incident-response procedures. Employees must not attempt to investigate or remediate suspected AI security incidents independently.
- **Vendor Security Review:** Departments seeking to adopt new AI tools must submit them to IT for security review prior to use. IT will evaluate vendor data-handling practices, contractual data protections, and alignment with City security standards.
- **Third-Party AI Risk:** AI tools operated by third-party vendors under contract with the City are subject to the City's standard data-security and vendor-management requirements. Departments must not grant third-party AI vendors access to City systems or data without IT and legal review.

12. Training, Governance, and Support

The City may provide training on responsible AI use, confidentiality, cybersecurity, public-records obligations, and specific tools such as Microsoft 365 Copilot. Departments with higher-risk data or use cases may receive role-specific guidance.

IT may not be able to provide technical support for AI tools not approved or provided by the City. Employees using unapproved tools do so without City support are in violation of this Policy.

The City IT Department including the City's IT consultant, in coordination with the City Manager's Office and Law Department, will serve as the primary governance body for AI use, including reviewing requests for new AI tools, evaluating AI agents and workflows, and maintaining the approved-tools list.

13. 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 logs, outputs, prompts, and associated practices to assess risk, effectiveness, and compliance.

This Policy will be reviewed periodically and updated as necessary to reflect changes in technology, law, regulatory guidance, and City operations. Employees are responsible for complying with the most current version of this Policy and any supplemental guidance issued by IT or the City Manager's Office.

14. 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 the nature and severity of the violation. Misuse involving High Sensitivity Data, resident data, deception, fabricated media, unauthorized automated communications, or security violations may also lead to civil or criminal legal action.

Employees who are uncertain whether a proposed use of AI is permitted under this Policy should contact their supervisor, the IT Department, or the City Law Department before proceeding.

Questions regarding this Policy should be directed to the City IT Department or City Manager's Office.

0127196.0607946 ~~4901-4381-87104901-5039-2522~~v1