The City of Alpharetta Information Technology Policy	No: 2.2
Acceptable Use of Artificial Intelligence Technology	Updated: March 2026
	Issued By: DIT Security Team Owner: ditsecurity@alpharetta.ga.us

1 Purpose and Benefits

The purpose of this acceptable use policy is to outline the principles and guidelines for the acceptable use of Artificial Intelligence (AI) technologies within The City of Alpharetta in accordance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The primary objective is to establish a secure and responsible approach to the procurement and use of Artificial Intelligence technologies to ensure the confidentiality, integrity, and availability of information. This policy is designed to promote the innovative use of Artificial Intelligence tools while also minimizing the potential for intentional or unintentional misuse, unethical outcomes, potential biases, inaccuracy, and information security breaches. The Artificial Intelligence Acceptable Use Policy addresses the use of artificial intelligence tools in government operations, particularly as it pertains to the handling of sensitive data and City information within these tools.

Major security concerns with the use of Artificial Intelligence include the presentation of untruthful and biased information, the unauthorized use of outside or unapproved technology to complete assigned tasks, and the potential disclosure of information used as an input to Artificial Intelligence software adding to the collective knowledge of the Artificial Intelligence software, etc. All use of Artificial Intelligence tools must comply with applicable City policies and legal requirements

Major security concerns with the use of Artificial Intelligence include the presentation of untruthful and biased information, the breach of employment contract by utilizing outside and unapproved technology to complete assigned tasks, information disclosure due to any information used as an input to Artificial Intelligence software adding to the collective knowledge of the Artificial Intelligence software, etc.

2 Authority

The City of Alpharetta, through the Department of Information Technology and City Administration, reserves the right to amend, curtail, or otherwise revise this policy at any time, and to change and enforce it for all employees, vendors, and persons doing business with the City.

All employees must acknowledge receipt of the City of Alpharetta Employee Manual and Benefits Handbook (Handbook) upon hire and periodically throughout employment. The Handbook provides a summary of employee benefits, personnel policies, and employment rules in effect at the time of publication. Information Technology policies are referred to in the Handbook but are maintained in a separate document with detailed provisions. By acknowledging the Handbook, employees also acknowledge and agree to be bound by the City's Information Technology policies.

3 Scope

This policy applies to all departments, employees, vendors, volunteers, contractors, and third-party users who can access Artificial Intelligence tools and technologies. The term "users" will reference everyone within this Scope.

4 Policy

Users and departments shall submit for review all software, applications, tools, and services utilizing Artificial Intelligence for City business operations before procurement. All users shall follow established policies and standards to implement technology resources using Artificial Intelligence.

The department director or their designee must evaluate all generated content intended for public use before publication, and the Artificial Intelligence tool must be attributed to it.

5 Authorized Use

- Purpose: Artificial Intelligence tools may only be used for legitimate and authorized purposes related to the mission and objectives of The City of Alpharetta, as determined by the Director of Information Technology.
- Compliance: Users must comply with all applicable laws, regulations, ethical standards, and City policies when utilizing Artificial Intelligence, including any requirements for PII, PCI, HIPAA, and CJIS data, data retention, or open-records laws.
- Control: No City data or records, including inputs or prompts, will be used for training or parameter tuning for Artificial Intelligence models outside the City's control. Artificial Intelligence technologies that cannot prevent City data or records from contributing to their language models are prohibited.

6 Allowed and Prohibited Technologies:

- Allowed AI: Artificial Intelligence tools approved by the Department of Information Technology. Microsoft Copilot for GCC is specifically designed for governments and is approved. Apple Intelligence is only allowed when used from a managed City iPhone or iPad that has City controls applied. Care must be given when using Adobe's Generative AI tools with Acrobat and Creative Cloud applications to avoid inputting personal information or information prohibited in this document. For a complete list of Approved Technology, please see the link in Section 16 below.

- Prohibited AI: The use of ChatGPT, DeepSeek, Gemini, DeepL, and other language models is prohibited unless a written request is submitted by the Department Director for consideration and approval by the Director of Information Technology

7 Procurement

- Procurement: All requests must be submitted to the Department of Information Technology before purchasing using the "I have an idea for new technology" option in the helpdesk system. The department will review and evaluate requests with the user and their department leadership.
- Required Information: The request must include the Artificial Intelligence technology used, what models or agents are deployed, what information was used to teach the model, how the model will be used, expected inputs and outputs, and how the user will ensure the system is capturing all inputs, including conversations leading to an output. Additional information may be required as part of the review process.

8 Acceptable Use

8.1 Data Privacy and Confidentiality

- Privacy Considerations: Artificial Intelligence applications shall not be used to process or generate content that violates individual privacy rights or confidentiality agreements.
- Sensitive Information: Users must exercise caution when using Artificial Intelligence tools with sensitive information and adhere to data protection policies, regulations, and laws.
- Any confidential or sensitive data is prohibited from being input into Artificial Intelligence tools or models.
- No City records or data that contain HIPPA, PCI, or CJIS information may be used to generate content via Artificial Intelligence. This restriction is in place to protect sensitive and confidential information, ensure compliance with applicable laws and regulations, and safeguard the privacy and security of individuals and the City.
- No City records or data may be used to generate content via Artificial Intelligence, including in writing prompts or training Artificial Intelligence models, without the consent of the Director of Information Technology.

8.2 Ethical Use:

- Bias and Fairness: Users should be aware of potential biases in Artificial Intelligence models and take measures to address and mitigate bias when using such tools. Artificial Intelligence models may produce output that utilizes bias via stereotypes, inaccurate data, or historically biased or discriminatory data, and it is the user's responsibility to evaluate and verify that the generated content is fair and without bias or discriminatory characteristics.
- Accountability: Individuals using Artificial Intelligence are responsible and accountable for the ethical implications of their generated content.
- Human-In-The-Loop (HITL): Artificial Intelligence tools, including Generative Artificial Intelligence and other automated decision-making systems, are prohibited from

being the only agents involved in any decision-making. By keeping a "Human-In-The-Loop" approach, Artificial Intelligence systems can be properly kept in check.

- Example: While the Human Resources department may consult with Artificial Intelligence platforms in making hiring decisions, it may not use Artificial Intelligence to scan and reject resumes automatically.
- Example: While the Public Works Department may consult with Artificial Intelligence platforms to analyze traffic flow or optimize maintenance schedules, it may not rely solely on Artificial Intelligence to make decisions about road closures or project prioritization without review by a qualified and trained human.

8.3 Security Measures:

- Access Controls: Access to Artificial Intelligence tools are restricted to authorized users based on job roles and responsibilities. Any attempt to circumvent access controls is strictly prohibited.

8.4 Records Retention:

- Auditability: Users who utilize Artificial Intelligence must maintain or be able to retrieve and provide a list of prompts and/or inputs used. This information shall be provided when requested by the City Clerk's Office for public disclosure policies and procedures.
- Meeting Transcripts: Artificial Intelligence tools used to capture and summarize meetings (virtual or not) create records subject to state records retention laws and must be retained. Users must use caution in meetings where a record will be created, and are encouraged to disable transcription when appropriate. Meeting participants shall be notified in advance when transcription is in use to ensure transparency.

8.5 Intellectual Property:

- Ownership: Users must respect intellectual property rights and ensure that the use of Artificial Intelligence does not infringe on copyrights, patents, or other proprietary rights.
- Attribution: When used to produce a final product, attribution of the Artificial Intelligence system is required. Any intellectual property that utilizes a high percentage (greater than 30%) of Artificial Intelligence-generated content must include comments in the documentation attributing the development to the Artificial Intelligence technology.
- All images, audio, and video generated using Artificial Intelligence must include credit acknowledging the use of Artificial Intelligence as a source.
- Any text or document generated via Artificial Intelligence must attribute the Artificial Intelligence system as a utilized technology or document author.
- All attributions should include an employee assertion (including the department or group who reviewed/edited the content).
    - Example: Some material in this brochure was generated using Copilot and was reviewed for accuracy by a member of the Department of Finance before publication.

8.6 Training and Awareness:

- Training: Users are suggested to undergo training on the responsible and secure use of Artificial Intelligence, including awareness of potential risks and ethical considerations.
- Reporting: Any concerns regarding Artificial Intelligence's misuse or ethical implications must be promptly reported to the Departments of Information Technology or Human Resources.

9 Compliance

This policy, including any future updates, shall take effect upon publication. Compliance is expected with all City policies and standards. Policies and standards may be amended at any time and without prior notice.

- The Department of Information Technology will conduct frequent compliance audits to ensure compliance with the outlined policies and standards.
- Violations of this Policy may result in disciplinary action up to and including immediate termination of employment as well as possible civil liabilities or criminal prosecution. Where appropriate, the City may advise legal officials or appropriate third parties of policy violations and cooperate with official investigations. The City will not retaliate against any individual who reports suspected policy violations or participates in an investigation in good faith.

10 Policy Exceptions

If compliance with this policy or standard is not feasible or technically possible, or if deviation from this policy in full, or in part, is necessary to support a City business function, users shall submit a written request for an exception to the Director of Information Technology. The request should specifically state the scope of the exception, along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the Information Technology Department, initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein. The Director of Information Technology shall review such requests and confer with the requesting department.

11 Termination and Business Continuity

The City Administrator or Director of Information Technology may order the termination of use of any Artificial Intelligence tool that has been found to generate outputs that cause a risk to data privacy and security, reputational damage to the City, or malicious consequences. The department or user shall immediately decommission the tool, conduct an investigation to determine the appropriate actions, and submit the corrective plan to their Department Director and the Director of Information Technology.

To minimize disruptions in service resulting from an immediate decommission, departments shall develop and maintain a contingency plan for business operations and functions utilizing Artificial Intelligence tools.

12 Definitions of Key Terms

Term	Definition
Generative AI	Generative Artificial Intelligence refers to a certain class of software, systems, or functionality provided by a combination of the two characterized by the utilization of large data and language models, algorithms, machine learning, and deep-learning models to mimic human intelligence. Such technology can generate original content such as images, text, audio, and video utilizing patterns and structured input data called "prompts". These also include systems capable of ingesting input and translating that input into another form, such as text-to-code systems.
Prompt	Structured input data that utilizes simple or complex instructions to generate content from Generative Artificial Intelligence technology.
PII	Personally Identifiable Information (PII) is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples of PII include names, social security numbers, biometric data, and other identifiers that can be used to identify someone.
PCI	PCI stands for Payment Card Industry. PCI Data Security Standards are national standards issued by the Payment Card Security Standards Council and apply to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. PCI also applies to all other entities that store, process or transmit cardholder data or may have an impact on the security of the cardholder data environment.
HIPPA	The Health Insurance Portability and Accountability Act, or, more simply, HIPAA, is a law that works to protect the medical information of U.S. citizens.
CJIS	CJIS stands for Criminal Justice Information Services, which is a division of the FBI responsible for the collection, warehousing, and dissemination of criminal justice information. It provides a range of tools and services to law enforcement and other agencies. Established in 1992, CJIS plays a crucial role in

	supporting criminal justice operations at local, state, and federal levels.
AI Parameter Tuning	The process of adjusting the hyperparameters of a machine learning model to optimize its performance. Hyperparameters are the settings or configurations that are set before the learning process begins and are not learned from the data. These include parameters like learning rate, batch size, number of layers in a neural network, and the number of units in each layer.

13 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

ditsecurity@alpharetta.ga.us

14 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	**Description of Change**	**Reviewer**
June 2025	Revisions to Draft	Montgomery, Adam
October 2025	HR Review	Randall, Cris
February 2026	Advisory Committee Review	Advisory Committee
March 2026	Final Review	Montgomery, Adam

15 NIST Cybersecurity Framework Functions

Identify	Protect	Detect	Respond	Recover
	PR.AC-3 PR.MA-2			

16 Related Documents

National Institute of Standards and Technology AI Risk Management Framework

National Institute of Standards and Technology Trust and Artificial Intelligence (Brian Stanton and Theodore Jensen)

GA GTA | Artificial Intelligence Responsible Use (SS-23-002) | Enterprise Policies, Standards, and Guidelines

GA GTA | Guidance for State Organizations | Office of Artificial Intelligence

Alpharetta SharePoint - Approved Technology - All Employees