ADMINISTRATIVE POLICIES

SECTION: 600 – Information Technology	**POLICY#:** 607
TITLE: Artificial Intelligence Acceptable Use Policy	**R & O #:** 23-58
	IMPLEMENTED BY PROCEDURE #: 607-A
SPONSORING DEPT/DIV: Department of Information Technology Services (ITS)	
ADOPTED: 09/26/2023	**REVIEWED: 2/12/2026**

BACKGROUND:

Generative Artificial Intelligence (GenAI) systems, when used intentionally and responsibly, can enhance data-informed decision-making, improve operational efficiency, and deliver timely, responsive services to the community. This policy establishes principles and guidelines for the ethical and practical use of AI technologies within County government.

PURPOSE:

This Policy establishes procedures and guidelines that:

1. Specify the County's strategic position on the use of GenAI Applications and models used in support of conducting County business and in accordance with applicable local, state, and federal laws.
2. Maintain confidentiality, integrity, and availability of information used and generated by GenAI systems.
3. Define the objectives for the County's usage of GenAI systems.
4. Define roles and responsibilities related to the County's usage of GenAI systems.

APPLICABILITY:

This policy and related implementing procedures apply to all individuals who use or connect to the County's network and systems, including but not limited to elected officials, employees, volunteers, interns, consultants, and contractors (collectively referred to herein as 'Workforce members').

AUTHORITY:

This Policy will be administered by the County Administrative Office in accordance with the authority delegated to the County Administrator in Washington County Code Section 2.04.100.

DEFINITIONS:

Generative AI (GenAI) is software that generates new content—such as text, images, audio, or video—based on user input. It utilizes machine learning and large language models to respond to prompts and can be found in tools like ChatGPT, Copilot, Gemini, and is integrated into Microsoft Office or Bing.

GenAI system or AI solution: Any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

County Solution Sponsor (CSS): A department or division representative who sponsors a cloud-hosted solution.

Department technology sponsors and custodians: A department or division representative who sponsors the technology solution (non-cloud-based).

Restricted: Information or data is classified as restricted when the unauthorized disclosure, alteration, and/or destruction of that data could cause a critical level of risk to the County. Protected or Sensitive Data is classified as Restricted Data. If this data is lost, compromised, or disclosed without authorization, it could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

CIS Controls: The County uses the Center for Internet Security (CIS) Controls to guide its cybersecurity practices. These controls are a set of recommended actions that help protect systems and data from cyber threats. By following the CIS Framework, the County works to keep its information secure and reduce risk.

GENERAL POLICY:

This policy guides the safe and effective use of GenAI in County operations. All workforce members must follow the rules and responsibilities.

POLICY GUIDELINES:

Any County Department seeking to purchase and/or operate a GenAI system must comply with the following:

- Follow the County Technology Acquisition requirements as defined in County Policy No. 605/Procedure 605-A Acquisition of IT Solutions.
- Undergo Cloud Service Review facilitated by the ITS. ITS will assess the risk of the potential GenAI system and conduct additional review steps as required by County Policy No. 606 Cloud Service Policy.
- Ensure that all GenAI used by the County or on its behalf adhere to the guiding principles of accuracy, transparency, equity, accountability, utility, and privacy.
- Establish and maintain processes to assess and manage risks presented by GenAI used by the County.
- Align governance of GenAI with existing security and privacy measures in accordance with the following County Administrative Policies:

- Policy 605 Acquisition of IT Solutions, and its procedure document.
- Policy 602 Information Technology Acceptable Use Policy.
- Policy 208 Management, Preservation, and Storage of Electronic Public Records.
- Policy 501 HIPAA Privacy for rules specific to the Health Insurance Portability and Accountability Act.
- County Policy No. 606 Cloud Service Policy

- Comply with the "Prohibited Uses" of GenAI systems section of this policy
- Support compliance with applicable laws and regulations.

Responsibilities:

- The County Administrator is responsible for determining whether or not the County will use GenAI.
- County Department Directors are responsible for ensuring that their workforce members follow this policy and any associated procedures or guidelines associated with any GenAI solution.
- County Counsel is responsible for advising on any legal issues associated with GenAI usage by or on behalf of County Departments.
- The Chief Information Officer (CIO) is responsible for ensuring that GenAI solutions are used in accordance with Policy 605 Acquisition of IT Solutions, and its procedure document, County Policy No. 602 Information Technology User Policy, and No. 606 Cloud Services Policy. If notified by the County contract administrator, the CIO may decide to alter or cease use of the GenAI solution if it is causing harm or an unacceptable level of risk.
- Each County department has an assigned Privacy Manager (PM). The PM supports the Department Director by ensuring that GenAI systems are used in accordance with the County's Policy 501: HIPAA Privacy.
- Each County department has an assigned Data Security Officer (DSO). The DSO supports the Department Director by ensuring that GenAI systems are used in accordance with the County's Policy 506: Personal Information Protection Policy.
- Each County department has an assigned Public Records Officer (PRO). The PRO supports the Department Director by ensuring that GenAI systems are used in accordance with the County's Policy 208: Management, Preservation and Storage of Electronic Public Records, Including Electronic Mail Correspondence.
- The Information Security Officer (ISO) is responsible for overseeing this policy, the County's usage of technology in compliance with the County's Policy 501: HIPAA Privacy and 606 Cloud Services Policy. The ISO is also responsible for overseeing the cybersecurity practices of GenAI used by or on behalf of the County Departments.
- ITS will ensure that the relevant CIS controls for acquired GenAI technology are in place to protect the availability and integrity of data stored in these systems.

- The County Finance Department is responsible for overseeing County contracting and procurement.
- County contract administrators are responsible for ensuring that the GenAI solutions and their vendors comply with County policies through contractual agreements. The County contract administrator is responsible for assessing and addressing the value and risk of the procured GenAI. They will notify ITS if the GenAI solution causes harm or an unacceptable level of risk that outweighs the value.

Prohibited Uses:

The use of certain GenAI systems is prohibited because they handle sensitive information, and there is a higher risk that they may cause harm. This includes the following prohibited purposes:

- Real-time and covert biometric identification.
- Emotion analysis, or the use of computer vision techniques to classify human facial and body movements into certain emotions or sentiment (e.g., positive, negative, neutral, happy, angry, nervous).
- Fully automated decisions that do not require any meaningful human oversight but substantially impact individuals.
- Social scoring, or the use of algorithmic systems to track and classify individuals based on their behaviors, socioeconomic status, or personal characteristics.
- Cognitive behavioral manipulation of people or specific vulnerable groups.
- Fully autonomous weapons systems or any system that does not align with County values.
- Information categorized by the County as "Restricted."

County workforce members must not submit any restricted or confidential information about members of the public or other workforce members to a GenAI system without prior written consent from their Department Director.

If County workforce members become aware of an instance where a GenAI system has caused harm, workforce members must report the instance to their supervisor and the Information Security Division at infosec@washingtoncountyor.gov.

Personal Use:

In compliance with County Policy No. 602 Information Technology User Policy, Workforce members shall not use personal GenAI accounts to conduct County business. Additionally, workforce members shall not store any County business-related information in a GenAI system they created for personal use, nor shall they store personal documents or data in a GenAI system created for County business purposes.

Exceptions:

Exceptions to this policy may only be granted by the County Administrator or their designee.

Implementation:

Elected officials and department directors are expected to be knowledgeable of, and shall be responsible for, implementing this policy within their respective departments. Observance of this policy is mandatory for all County employees, and violation may result in disciplinary action (up to and including termination).

Periodic Review:

This policy shall be reviewed every two years, or more often, based on changes to the County's risk landscape and new and emerging cyber threats.