

Artificial Intelligence (AI) Acceptable Use Policy

INTRODUCTION

Utilizing AI can provide HOSWWA with the potential to automate tasks, improve decision-making, speed production of documents, create messaging content, and provide valuable insights into our operations. However, the use of AI also presents challenges and risks in terms of data and information security.

PURPOSE

The purpose of the Artificial Intelligence Acceptable Use Policy is to guide HOSWWA representatives with the safe, secure, and ethical use of AI, safeguarding the confidentiality and integrity of agency and client data while mitigating unauthorized access or breach of the same. The policy provides educational background on AI and outlines HOSWWA's requirements with respect to the adoption of all forms of artificial intelligence at the agency.

SCOPE

This policy applies to all HOSWWA representatives and identifies approved AI technical systems as identified in Addendum A.

DEFINITIONS

Artificial Intelligence (AI): Defined as the use of machine learning technology, software, automation, and algorithms to perform tasks and make rules or predictions based on existing datasets and instructions.

Generative AI: Deep-learning models that can generate high quality text, images, or other content based on the data they have been trained on. This includes chatbots such as ChatGPT, Google (and other search engines) Gemini, Microsoft Copilot, or text-to-image models such as Stable Diffusion or Midjourney.

Approved AI Technical System(s): Software, platforms, and any other form of Artificial Intelligence (AI) system that the CEO has approved for use by HOSWWA. Please see Addendum A.

Personally Identifiable Information (PII): Protected personal information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Non-public HOSWWA Data: Any information that, if disclosed, could violate the privacy of individuals, government regulations or statutes, could jeopardize the financial state of HOSWWA, could injure its reputation, or could reduce its competitive advantage.

HOSWWA Representative: All HOSWWA employees, board members, contractors, representatives, affiliates or agents that are utilizing HOSWWA systems to produce information for the agency.

POLICY

While HOSWWA understands the potential benefits of utilizing AI, the use of AI should never compromise HOSWWA core values or introduce undue risk on the agency. The use of AI can be risky especially in terms of data security. Additionally, the use of AI has shown to perpetuate biases and barriers and therefore the use of these systems in our daily work must be carefully considered.

There are additional considerations due to our status as a public agency. As a government agency we are required to retain all records created for the performance of our work, meaning that stored input into an AI system will be considered a record that must be retained for the Washington Public Records Act.

AI Technical Systems are approved by the CEO after careful consideration of risk and exposure. As part of the approval process for any new AI system, the IT Coordinator will reach out to the IT Administrators to evaluate the AI system for potential risks to our systems. HOSWWA representatives must only use AI tools that have been vetted to meet our security and data protection standards. The list of approved resources may be found in **Addendum A**.

When considering use of AI for a business task or process, all employees should verify that the use coincides with approved uses detailed in this policy or does not violate any of the prohibited uses. Therefore, any employee considering the use of AI for a task or process should first check in with their supervisor to ensure that this is an approved use. Guidance is provided below in the Prohibited, Low Risk and High-Risk sections to assist in making these decisions.

While AI tools are valuable tools for efficiency in the workplace, they should not be treated as authoritative or infallible. AI tools construct responses based on learned patterns from an array of resources. The responses may not be 100% accurate. Therefore, all information retrieved from an AI tool must be reviewed for accuracy and completeness.

Any employee that becomes aware of prohibited AI use within the workplace (including on personal phones) or unauthorized AI systems added to HOSWWA computers is required to notify their supervisor immediately.

HOSWWA as a government entity must conduct its operations in a way that upholds public trust. Therefore, there are areas of our operations where AI usage will be strictly prohibited as follows:

AI Prohibited Use

- Employees are prohibited from using AI to assist with managing or processing any housing waitlists.
- Employees are prohibited from using AI to assist with screening or processing applications for housing, employment or any other area where an employee decides on the outcome of a person's housing, employment or other important matters.
- Employees are prohibited from using AI to generate any ads for housing through digital platforms.

- Employees shall not input, upload or enter in AI systems any internal HOSWWA documents (completed or in draft form) such as contracts, applications, legal documents or other documents that can be identified with the agency and would not be findable by the public using an internet search.
- Employees shall not enter any personal identifiable information as AI input data.
- Employees shall not enter any identifying characteristics of a specific person (disability status, race, gender, marital status, etc.) as AI input data.

All of the above applies to any AI system including google and other search engines as defined in the definitions section.

The following are High-Risk uses of AI and may only be used with supervisor approval:

- Using an AI tool or system to obtain legal advice.
- Inputting any personal (non PII) data into an AI System.
- Requesting data or statistics from AI—incomplete or inaccurate data is added to AI systems for testing. Therefore, any data pulled from AI must be verified by a secondary source.
- Downloading documents from AI can include Malware. Caution Advised!

The following are Low-Risk uses of AI and may be utilized on HOSWWA approved AI systems:

- Getting assistance drafting an email that does not include any Personally Identifiable Information.
- Drafting a form with no proprietary information.
- Drafting presentation documents with no proprietary or personally identifiable information.
- Assistance with phrasing that does not compromise data.
- Working on raw unidentifiable data or numbers in word or excel documents.

Training

All managers will be trained in the proper use of generative AI tools in the workplace. Managers are required to take Breach Secure Now Artificial Intelligence (AI) for Managers Training.

All employees using AI tools for work purposes must attend Breach Secure Now Artificial Intelligence (AI) Awareness Cybersecurity Training on the proper use of these technologies before doing so.

All questions related to this training should be addressed to the IT Coordinator or CEO.

Disciplinary Action

Any HOSWWA representative utilizing AI as prohibited by the AI Prohibited Use section or utilizing prohibited AI under Addendum A is subject to disciplinary action or termination. HOSWWA representatives are expected to be extremely cautious when engaging in High-risk AI usage and expected to use good judgment when engaging in Low-risk AI usage. Failure to do so may result in disciplinary action or termination.

When considering use of AI for a business task or process, all employees should verify that the use coincides with approved uses detailed in this policy or does not violate any of the prohibited uses. Therefore, any employee considering the use of AI for a task or process should first check in with their supervisor to ensure that this is an approved use. Guidance is provided in the Prohibited, Low-Risk and High-Risk sections to assist in making these decisions.

Addendum A

Approved AI Technical System(s)

The list of **approved** AI technical systems includes:

Name	Website	Approved Use
Copilot	Accessed through Microsoft 365	Idea formulation, general content creation
Canva	www.canva.com	Creation of brochures, newsletters, posters, etc., without uploading proprietary information.
Scribe	Account Access through Business Analyst	Creation of SOP's
Zoom	https://www.zoom.com/	AI note taking for Board Meetings

The list of **prohibited** AI technical systems includes:

Name	Website	PROHIBITED ACCESS
ChatGPT	www.chatgpt.com	DO NOT USE ON AGENCY SYSTEMS
Claude	https://claude.ai	DO NOT USE ON AGENCY SYSTEMS