

# Privacy Webinar: Artificial Intelligence

---

August 29, 2023

Office of Privacy and Data Protection

Katy Ruckle, State Chief Privacy Officer

Nick Stowe, State Chief Technology Officer

Irene Vidyanti, State Chief Data Officer

- WaTech's Role
  - CTO
  - CDO
  - CPO
- AI Community of Practice
  - Governance
  - Initiatives
- Generative AI Guidelines
- What's next?

# WaTech's Role

## WaTech's Role

- RCW 43.105.205
  - "To **educate** and **inform** state **managers** and **policymakers** on **technological developments**, industry **trends** and **best practices**..."
  - "To **establish standards** and **policies** for the consistent and efficient operation of information technology services...."
- Enterprise responsibility
  - RCW 43.105.265 "...shall develop an **enterprise-based strategy** for **information technology** in state government"

# State Chief Technology Officer

- Who are you?
  - Nick Stowe, Washington State Chief Technology Officer
  - Also - **Washingtonian, Dad, Nerd, Technology Enthusiast**
- What does the State CTO for Washington State do?
  - Leadership, vision, and execution of enterprise technology programs and initiatives focused on **architecture, data, cloud, innovation, and emerging technology**
- What is your role in relationship to AI?
  - Co-Chair for the AI Steering Committee
  - **Align AI** applications with **business, technology, and risk** management strategies
  - **Encourage collaboration** between public sector organizations, **promote** strategies for technology **re-use**



# State Chief Data Officer x AI - in 3 panels

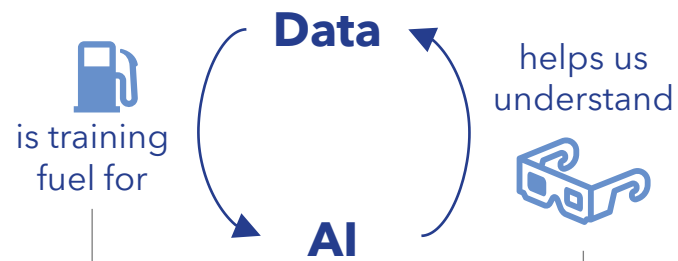
Who are you?



Irene Vidyanti  
State Chief Data Officer

Role: Provide leadership, vision, and execution for the enterprise data program

What is the relationship between AI & data?

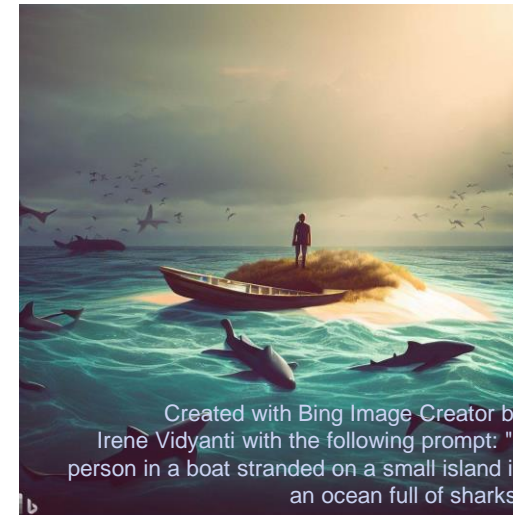


AI only as good as data it was "fed" → Need to address data challenges, from quality to equity

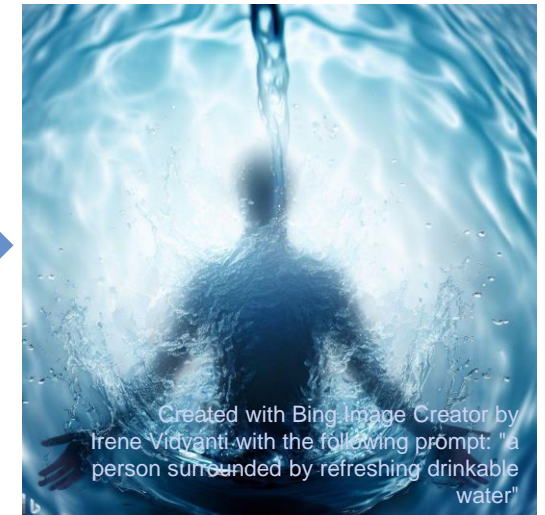
AI helps us understand patterns in data → Need to improve data literacy

What is your role in relationship to AI?

Data, data everywhere  
**Not a drop of insight to drink**



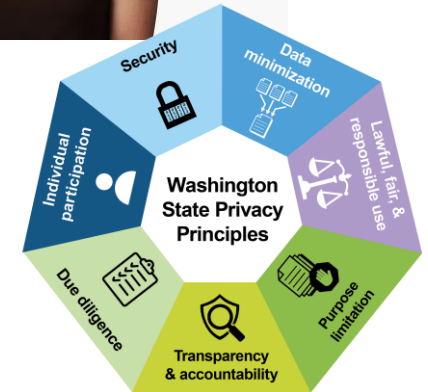
Data, data everywhere  
**An abundance of actionable insights to gain**



Enterprise Data will propel WA State along this continuum

# State Chief Privacy Officer

- Who are you? Katy Ruckle, State Chief Privacy Officer
- What does CPO do? Position created in RCW 43.105.369 –
  - Privacy Principles
  - Projects that involve personally identifiable information (PII)
  - Data Protection
- What is CPO role in relationship to AI?
  - Automated Decision Systems Work
  - Generative AI



# AI Community of Practice



## AI CoP

- **Governance Structure**
  - Representation from WaTech, State Agency, and Local Government
- **Steering Committee Objectives**
  - Develop a set of **guidelines** and **policies**
  - Identify and document **best practices**
  - Establish a **governance structure** and develop mechanisms for accountability and oversight
  - **Document use cases** and examine potential societal impact
  - **Facilitate collaboration** and knowledge sharing
  - **Promote alignment** of new AI technologies to business and IT strategies



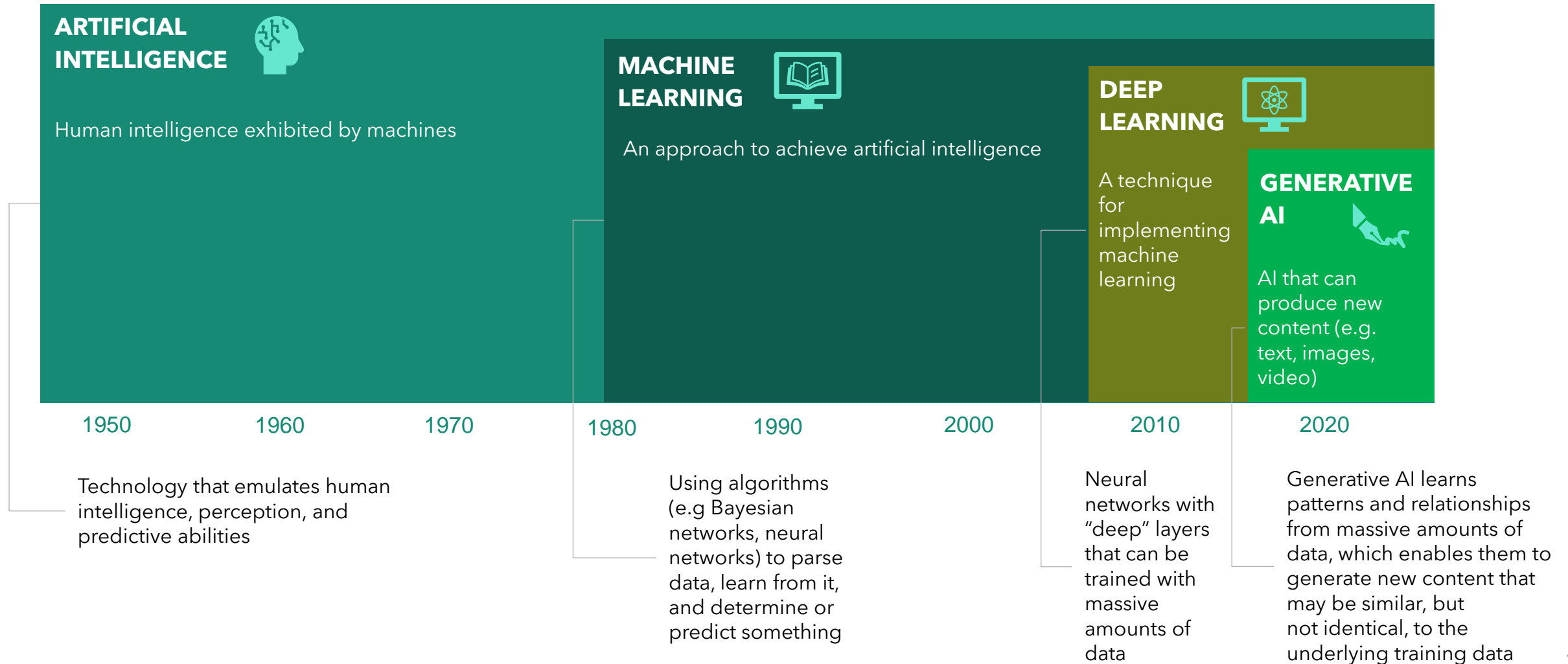
# AI CoP Current Initiatives

- Feedback on interim Generative AI guidelines
- Establishing Subcommittees to support areas of interest (risk, use cases, local government)
- Information sharing on industry evolution of Generative AI



# Generative AI Guidelines

## What are we talking about?



# <https://ocio.wa.gov/policy/generative-ai-guidelines>

- Interim Guidelines for Purposeful and Responsible Use of Generative Artificial Intelligence
  - Background
  - Definition
  - Principles
  - Guidelines
  - Generative AI Usage Scenarios and Dos and Don'ts
  - Use Cases
  - Acknowledgments



## Background

The rapid advancement of generative artificial intelligence (AI) has the potential to transform government business processes, changing how state employees perform their work and ultimately improving government efficiency. These technologies also pose new and challenging considerations for implementation.

These guidelines are meant to encourage **purposeful and responsible use** of generative AI to foster public trust, support business outcomes, and ensure the ethical, transparent, accountable, and responsible implementation of this technology.

This document serves as an initial framework for the responsible and ethical use of generative AI technologies within the Washington state government. Recognizing the rapidly evolving nature of AI, these guidelines will be periodically reviewed and updated to align with emerging technologies, challenges, and use cases.

## Definition

[Generative Artificial Intelligence \(AI\)](#) is a technology that can create content, including text, images, audio, or video, when prompted by a user. Generative AI systems learn patterns and relationships from massive amounts of data, which enables them to generate new content that may be similar, but not identical, to the underlying training data. The systems generally require a user to submit prompts that guide the generation of new content. (Adapted slightly from [U.S. Government Accountability Office Science and Tech Spotlight: Generative AI](#))

## Principles

The intention of the state of Washington is to follow the principles in the [NIST AI Risk Framework](#), which serve as the basis for the guidelines in this document. A foundational part of the NIST AI Risk Framework is to ensure the trustworthiness of systems that use AI. The guiding principles are:

- **Safe, secure, and resilient:** AI should be used with safety and security in mind, minimizing potential harm and ensuring that systems are reliable, resilient, and controllable by humans. AI systems used by state agencies should not endanger human life, health, property, or the environment.
- **Valid and reliable:** Agencies should ensure AI use produces accurate and valid outputs and demonstrates the reliability of system performance.

## Definition of Generative AI

- Technology that can create content:
- text, images, audio, or video
- Generative AI systems learn patterns and relationships from massive amounts of data, which enables them to generate new content that may be similar, but not identical, to the underlying training data.
- The systems generally require a user to submit prompts that guide the generation of new content.



# Guiding Principles for Generative AI Use



- **Safe, secure, and resilient:**

- AI should be used with safety and security in mind, minimizing potential harm and ensuring that systems are reliable, resilient, and controllable by humans.
- AI systems used by state agencies should not endanger human life, health, property, or the environment.

- **Valid and reliable:**

- Agencies should ensure AI use produces accurate and valid outputs and demonstrates the reliability of system performance.



- **Fairness, inclusion, and non-discrimination:**

- AI applications must be developed and utilized to support and uplift communities, particularly those historically marginalized.
- Fairness in AI includes concerns for equality and equity by addressing issues such as harmful bias and discrimination.

- **Privacy and data protection:**

- AI should be used to respect user privacy, ensure data protection, and comply with relevant privacy regulations and standards.
- Privacy values such as anonymity, confidentiality, and control generally should guide choices for AI system design, development, and deployment.
- Privacy-enhancing AI should safeguard human autonomy and identity where appropriate.

- **Transparency and auditability:**

- Acting transparently and creating a record of AI processes can build trust and foster collective learning.
- Transparency reflects the extent to which information about an AI system and its outputs is available to the individuals interacting with the system.

- **Accountability and responsibility:**

- As public stewards, agencies should use generative AI responsibly and be held accountable for the performance, impact, and consequences of its use in agency work.

- **Explainable and interpretable:**

- Agencies should ensure AI use in the system can be explained, meaning “how” the decision was made by the system can be understood.
- Interpretability of a system means an agency can answer the “why” for a decision made by the system, and its meaning or context to the user

- **Public purpose and social benefit:**

- The use of AI should support the state’s work in delivering better and more equitable services and outcomes to its residents.

# Guidelines for Generative AI Use



## • **Fact-checking, Bias Reduction, and Review**

- All content generated by AI should be reviewed and fact-checked, especially if used in public communication or decision-making.
- State personnel generating content with AI systems should verify that the content does not contain inaccurate or outdated information and potentially harmful or offensive material.
- Given that AI systems may reflect biases in their training data or processing algorithms, state personnel should also review and edit AI-generated content to reduce potential biases.
- When consuming AI-generated content, be mindful of the potential biases and inaccuracies that may be present.

- **Disclosure and Attribution**

- AI-generated content used in official state capacity should be clearly labeled as such, and details of its review and editing process (how the material was reviewed, edited, and by whom) should be provided. This allows for transparent authorship and responsible content evaluation.
- State personnel should conduct due diligence to ensure no copyrighted material is published without appropriate attribution or the acquisition of necessary rights. This includes content generated by AI systems, which could inadvertently infringe upon existing copyrights.

- **Sensitive or Confidential Data**

- Agencies are strongly advised not to integrate, enter, or otherwise incorporate any non-public data (non-Category 1 data) or information into publicly accessible generative AI systems (e.g., ChatGPT).
- If non-public data is involved, agencies should not acquire generative AI services, enter into service agreements with generative AI vendors, or use open-source AI generative technology unless they have undergone a Security Design Review and received prior written authorization from the relevant authority, which may include a data sharing contract.
- Contact your agency's Privacy and Security Officers to provide further guidance.

## State Ethics law - Confidential Information

- [RCW 42.52.050](#)

(3) No state officer or state employee may disclose ***confidential information*** to any ***person*** not entitled or authorized to receive the information.

- Definitions ([RCW 42.52.010](#)):

(5) "Confidential information" means (a) specific information, rather than generalized knowledge, that is not available to the general public on request or (b) information made confidential by law.

(15) "Person" means any individual, partnership, association, corporation, firm, institution, or other entity, whether or not operated for profit.



# Generative AI Usage Scenarios Do's and Don'ts



## ✓ Do's (best practices) and ✗ Don'ts (things to avoid)

➤ **Rewrite documents in plain language for better accessibility and understandability.**

✓ **Do** specify the reading level in the prompt, use readability apps to ensure the text is easily understandable and matches the intended reading level, and review the rewritten documents for biases and inaccuracies.

➤ **Condense longer documents and summarize text.**

✓ **Do** read the entire document independently and review the summary for biases and inaccuracies.


✗ **Don't** include sensitive or confidential information in the prompt


## ➤ Draft Documents

✓ **Do** edit and review the document, label the content appropriately, and remember that you and the state of Washington are responsible and accountable for the impact and consequences of the generated content.

**X Don't** include sensitive or confidential information in the prompt or use generative AI to draft communication materials on sensitive topics that require a human touch.

## ➤ Aid in Coding

 **Do** understand what the code is doing before deploying it in a production environment, understand the use of libraries and dependencies, and develop familiarity with vulnerabilities and other security considerations associated with the code.

 **Don't** include sensitive or confidential information (including passwords, keys, proprietary information, etc.) in the prompt and code

➤ **Aid in generating image, audio, and video content for more effective communication**

✓ **Do** review generated content for biases and inaccuracies and engage with your communication department before using AI-generated audiovisual content for public consumption.

**x Don't** include sensitive or confidential information in the prompt.

## ➤ Automate responses to frequently asked questions from residents (example: chatbots)

✓ **Do** implement robust measures to protect resident data.

**X Don't** use generative AI as a substitute for human interaction or assume it will perfectly understand residents' queries. Provide mechanisms for residents to easily escalate their concerns or seek human assistance if the AI system cannot address their needs effectively.

## Other Use Cases



# Other data and privacy considerations for Generative AI?

Where did the training data come from?

Was the training data legally obtained?

Data being used as a proxy for something else?

---



# Artificial Intelligence Regulation in Washington

- **SSB 5116 (2021)** - Establishing guidelines for government procurement and use of **automated decision systems** in order to protect consumers, improve transparency, and create more market predictability.

POLICY

## Lawmakers Move to Ban Discriminatory Tech in Washington State

In response to reports detailing AI tech's disproportionate impact on communities of color, Washington State Sen. Bob Hasegawa introduced a bill to ban AI tech and regulate automated decision systems.

February 23, 2021 • Katya Maruri

**Questions?**

