

# ADMINISTRATOR'S MEMORANDUM

To: State Office and Regional Offices

Miscellaneous Memorandum No. 22

From: Mat Weaver, Director



Date: December 18, 2025

RE: Using Artificial Intelligence

---

*This document was created with assistance from ChatGPT. Specifically, ChatGPT was used to review and comment on the Statement of Policy and AI Use sections of this policy, which resulted in the modification of those sections. All information has been reviewed and edited for accuracy by IDWR's ITS Liaison Group.*

## Purpose

To establish an Idaho Department of Water Resources (IDWR) policy on the appropriate use of artificial intelligence (AI) and outline the steps staff must follow before using or publishing any AI-generated material.

## Definitions

For the purposes of this policy, "AI-generated information" refers to any material, content, summary, dataset, or image created wholly or in part with AI tools or technologies. "AI tools" and "AI technologies" refer to machine-learning computational technologies that simulate human intelligence (e.g., ChatGPT, Google Gemini, Microsoft Co-Pilot, etc.). Microsoft 365 tools and add-ins, such as spell check, as well as Excel formulas, are not considered AI tools.

## Background

AI is a wide-ranging technology that can create content when prompted by a user. AI tools can write, summarize, evaluate, illustrate, compose, code, and perform a range of other tasks. AI offers potential efficiency gains due to its ability to complete complex tasks quickly. IDWR employees are encouraged to consider and incorporate the use of AI into their daily work, where it can enhance efficiency and consistency in functions.

However, responsibly using AI and AI-generated content poses ethical, transparency, and accountability challenges, especially for government agencies. IDWR's employees must use AI in an ethical, responsible, and thoughtful manner.

The Idaho Office of Information Technology Services (ITS) has two publications that guide the responsible use of AI for state employees. These two publications can be reviewed for more in-depth consideration of this topic.

- [Idaho's AI Advantage: A Framework for Responsible Innovation, 2025](#)
- [Artificial Intelligence \(AI\): Governance, Policy, Standard, and Guidelines, August 2025](#)

In its guidance, ITS outlines eight core principles for the ethical and responsible use of AI.<sup>1</sup> The principles include:

1. Human-Centered Design: AI should be used to enhance human capability, not replace it.
2. Transparency and Explainability: If [AI tools are used to generate or modify substantive content (including public documents and information)], employees should disclose its use and be able to explain (in plain language) the AI system and prompts used, how and why the AI reached that decision, how outputs are used in decision making, and the limitations of the AI.
3. Appropriate Oversight: Supervision, peer review from subject-matter experts, and human judgment should review [substantive] AI-generated content and AI-automated decisions.
4. Fairness and Accessibility: AI must serve all Idahoans equally and without bias. Scrutinize AI systems and content for representation and balance before, during, and after publishing outputs.
5. Security and Privacy by Design: Minimize data collection by AI systems, implement consent mechanisms to clearly inform users of how their data will be used, and *never* enter personal or sensitive data into AI.
6. Risk-Based Governance: Scale review and oversight for AI according to the system's impact on people, data, and public trust.
7. Continuous Improvement: Routinely evaluate AI systems used, or AI content generated based on performance, stakeholder input, and shifts in best practices.
8. Shared Responsibility: Agencies and departments share responsibility with ITS to responsibly use and implement AI. ITS retains the authority to reject high-risk AI implementations.

IDWR must also keep in mind the following liabilities surrounding AI tools and information:

- AI information can be misleading, biased, or inaccurate based on how a prompt was written, the quality of data input, and the sources drawn from.
- AI tools can produce false or contradictory information, known as hallucinations.
- AI models may rely on historical data that may not be current.
- AI models can draw on all types of information, including opinion, speculation, and satire.
- AI models are built to take in and retain information, which could compromise sensitive information.

## Statement of Policy

To implement AI tools ethically and responsibly while minimizing AI's potential liabilities, IDWR staff members must adhere to the following standards when using AI tools:

---

<sup>1</sup> Refer to ITS publication *Idaho's AI ADVANTAGE A Framework for Responsible Innovation*, pp. 7-11.

1. Never enter personally identifiable information, protected health information, confidential enforcement actions, confidential attorney-client privileged information, information subject to a non-disclosure agreement, or any other sensitive information or data that would be exempt from a public records request into an AI tool.
2. Use of AI-generated information and tools should comply with all State of Idaho policies. This includes ITS' AI Governance Policy, Standard, and Guideline (P.ITS-01, S.ITS-01, and G.ITS-01).
3. Use of AI-generation must be confined to approved tools. Consistent with the December 16, 2025, recommendation from ITS, Microsoft Copilot is IDWR's preferred AI tool. Employees should use the version of Copilot embedded in Microsoft 365. Or, for more robust applications, IDWR may ask ITS to purchase a Microsoft 365 Copilot full business license, if staff submit a justified request and their managers approve it. If employees are interested in using another AI tool, such as Adobe AI Assist, Grammarly, or ChatGPT, they must get approval from their supervisor and the Regional Manager, Deputy Director, or Director who has executive management oversight for the employee and get approval from IDWR's ITS Liaison Group.<sup>2</sup>
4. Use of AI-generated information must be transparent.

Staff must prompt the AI tool to provide its sources and review the source material before incorporating AI-generated information into any public document.

Staff must add a disclosure statement to substantive content generated or materially modified using AI tools so that the recipient is aware of the AI systems involved. Substantive content includes content for IDWR's social media, website updates, and materials developed for public availability and accessibility.

Staff must use their best judgment when determining whether a disclosure statement is warranted. Below are two examples for guidance.

- Example 1: A fact sheet that will be posted on the website that was generated using AI should undergo a human review and include a disclosure statement.
- Example 2: A letter or email that was written by an employee and edited by an AI tool does not require a disclosure statement.

The disclosure statement must identify the AI-generated information, the AI tool used, and a statement noting that the information has undergone human review:

---

<sup>2</sup> IDWR's ITS Liaison Group is comprised of IDWR's ITS Service Delivery Manager, IDWR's Agency IT Business Analyst, and the Deputy Director overseeing agency operations. This group meets regularly to plan and coordinate ITS matters.

AI Usage Disclosure: This document was created with the assistance of [specify the AI tool]. All information has been reviewed and edited for accuracy by [author's full name].

5. AI-generated information must undergo human review.

A human must review all AI-generated information created for external use. Materials produced without the assistance of AI should still undergo a review as a best practice.

Human reviews must evaluate data and content for accuracy, objectivity, and fairness to ensure it aligns with IDWR's mission and legal obligations.

6. IDWR must follow data safety protocols when using AI tools.

Only Level 1 data can be entered into AI tools. This includes public information with minimal privacy or security concerns (e.g., information on the public website).<sup>3</sup> Entering Level 2, 3, and 4 data requires written approval from both a deputy director and the director.

**Table 1: Data Classification**

Data Classification			
Level 1   Unrestricted   Public	Level 2   Limited   Internal	Level 3   Restricted   Federal	Level 4   Critical
<ul style="list-style-type: none"><li>- Press releases</li><li>- Brochures</li><li>- Public websites</li><li>- Published research</li><li>- Materials created for public consumption</li></ul>	<ul style="list-style-type: none"><li>- Internal audit reports</li><li>- Financial transactions</li><li>- Emails</li><li>- Non-public phone numbers</li><li>- Building schematics</li><li>- Names and addresses that are not protected from disclosure</li></ul>	<ul style="list-style-type: none"><li>- Employee records</li><li>- Financial data</li><li>- Internal reports</li><li>- Personal contact details</li><li>- Social Security Number (SSN)</li><li>- Driver's license number</li><li>- Passport number</li><li>- Tax returns</li><li>- Fingerprint data</li><li>- Warrants or restraining orders</li><li>- Medical records</li><li>- Credit card numbers (PAN)</li></ul>	<ul style="list-style-type: none"><li>- Disclosure that could result in loss of life, disability, or serious injury</li><li>- Regulated information with significant penalties for unauthorized disclosure. This information is typically exempt from public disclosure</li></ul>

## AI Uses

All "Appropriate Uses" must adhere to items 1 – 6 in the Statement of Policy.

### Appropriate Use

- Generating ideas, outlines, or brainstorming options
- Drafting emails and internal correspondence
- Developing PowerPoint slide decks or presentation materials
- Drafting plain language summaries or technical or regulatory concepts for public communication

<sup>3</sup> To review ITS' data classification system, refer to its [Information Security Policy Manual v4.0](#), policy RA-02 Security Classification, pg. RA-124.

- Drafting outreach or education materials
- Drafting decision packets, briefing materials, or legislative summaries
- Drafting internal policies, procedures, or guidance documents
- Drafting letters, notices, and public information materials
- Summarizing nonconfidential meetings
- Conducting preliminary reviews of summaries of data
- Comparing, screening, or organizing documents
- Aggregating, summarizing, and compiling public comments
- Conducting initial completeness checks for applications or submittals
- Developing, modifying, and testing code, scripts, or data processing routines
- Analyzing, visualizing, or identifying trends or anomalies in datasets
- Extracting or classifying information from large document sets
- Summarizing technical reports, studies, or datasets to support decision making
- Assisting in quality assurance by checking formatting consistency, missing information, or template adherence

### **Inappropriate Use**

- Generating images, videos, or audio of others without their informed, written consent
- Generating tables or figures without validating underlying data sources and disclosing the use of AI
- Relying on AI-generated information for technical analyses, calculations, or quantitative results without thorough human review and validation
- Using AI to produce, edit, or format substantive content without human oversight and without citing or documenting the use of AI tools
- Publishing or releasing materials containing substantive AI-generated content without including a disclosure statement in public-facing documents
- Using AI instead of direct human collaboration or failing to inform other participants when AI tools are used in collaborative work
- Entering or uploading confidential, sensitive, proprietary, or non-public data into any AI tool that is not approved for such use or does not ensure adequate data security
- Allowing AI tools to draft, approve, or submit final agency decisions or official communications without human review and sign-off
- Using AI to generate or summarize formal legal interpretations, regulatory guidance, or compliance determinations without review by qualified staff or legal counsel
- Using AI tools that do not comply with state IT security, accessibility, or privacy standards
- Disclosing or incorporating personally identifiable information, tribal data, or other protected information into AI systems
- Engaging AI tools to impersonate specific agency employees, contractors, or members of the public

- Using AI outputs as sole evidence or justification for policy, management, or enforcement decisions

**Responsibility**

IDWR's ITS Liaison Group is responsible for maintaining this policy.

**Implementation**

This policy is effective immediately and will remain in effect unless amended, replaced, or rescinded prior to its expiration.