OREGON YOUTH AUTHORITY

Policy Statement

Part I – Administrative Services

Subject:

Use of Artificial Intelligence (AI)

Section – Policy Number:	*Supersedes:*	*Effective Date:*	*Date of Last Revision/Review:*
E: Information Management – 3.4	**N/A**	**06/22/2026**	**None**

Related Standards and References:	▪ Oregon's State Government Artificial Intelligence Advisory Council ▪ DAS Enterprise Information Services (EIS) Generative AI Access and Usage Guidance ▪ National Institute of Standards and Technology (NIST): Artificial Intelligence Risk Management Framework (AI RMF 1.0) NIST SP 1270 Towards a Standard for Identifying and Managing Bias in Artificial Intelligence ▪ OYA policy: 0-7.0 Use of Electronic Information Assets and Systems I-E-3.2 Information Classification and Protection I-E-3.3 Information Security Incident Response ▪ Attachment A: Data Classification Risk Model
Related Procedures:	▪ TS I-E-3.3 Service Desk Information Security Incident Response

Policy Owner:	**Approved:**
Chief Information Officer	Mike Tessean, Director

I. PURPOSE

This policy establishes OYA's allowable use of artificial intelligence (AI) in the workplace and aligns with statewide guidance from Oregon's State Government Artificial Intelligence Advisory Council, Enterprise Information Services (EIS), and OYA policy 0-7.0 Use of Electronic Information Assets and Systems.

II. POLICY DEFINITIONS

Artificial Intelligence (AI): A machine-based system capable of performing tasks such as making predictions, recommendations, or decisions that influence real or virtual environments. (The National Institute of Standards and Technology (NIST)).

AI transparency: Transparency and clarity surrounding the decision-making processes, algorithms, and data used in artificial intelligence systems. Transparency makes AI systems more understandable and accessible to stakeholders.

Generative Artificial Intelligence (GenAI): Umbrella term for technologies that synthesize content mirroring human creativity. Encompassing machine learning and language models, GenAI generates human-like text, audio, imagery, video, and other digital content. Generative AI poses significant risks, including misinformation, fake content, realistic fake videos, and audio recordings increasing concerns about the potential for manipulation.

High Risk AI: AI systems that are considered to pose a high risk to youth eligibility, placement, benefits, staff discipline, or legal rights, but whose benefits outweigh these risks.

III. POLICY

This policy provides guidance for applying AI in support of OYA's mission to advance youth rehabilitation; improve youth outcomes and staff services; protect the rights of youth, families, and staff; and comply with applicable laws and statewide policies.

All AI use cases must also comply with the EIS Artificial Intelligence Impact Assessment (AIIA) process, with Tier 2 and Tier 3 use cases submitted to the statewide repository for approval and reporting.

In accordance with Oregon's State Government Artificial Intelligence Advisory Council Final Recommended Action Plan, OYA must use the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (AI RMF 1.0) definitions for reference and consistency.

This policy applies to all OYA staff who design, acquire, configure, deploy, use, or manage AI capabilities on behalf of OYA. This includes:

- AI tools (including Generative AI) (e.g., Microsoft Copilot, ChatGPT);
- Embedded AI features in vendor products;
- Third-party AI services used in OYA operations or youth programs; and
- Embedded AI features for in-house application development.

For purposes of this policy, all restrictions and requirements apply equally to standalone AI tools and to embedded AI features within approved enterprise platforms (e.g., Microsoft Copilot, vendor-provided AI functionality).

Volunteer coordinators and contract administrators must ensure volunteers and contractors are aware of and comply with this policy.

IV. GUIDING PRINCIPLES

The below OYA AI Guiding Principles align with Oregon's State Government Artificial Intelligence Advisory Council.

A. Accountability: AI systems must be subject to continuous audits measuring fairness, accuracy, safety, and efficiency, with clear reporting to Oregonians.

B. Accessibility: All AI systems and outputs must comply with Section 508 and WCAG 2.1 accessibility standards to ensure equitable access for staff, youth, and the public.

C. Equity and Representation: AI systems must clearly explain decision-making processes to users and affected parties through accessible and transparent communication. The AI Ethics Review Board (AI-ERB) must apply an equity lens to all reviews, particularly assessing impacts on youth, families, and staff.

D. Explainability and Trust: AI systems deployed by OYA must be developed and implemented with transparent methodologies, data sources, and design procedures. Those asked to engage with AI or have their data used by AI may do so with informed consent. AI decision-making processes must be clearly explained to both users and affected individuals.

E. Governance: OYA policies, processes, procedures, and practices must be related to the mapping, measuring that managing of AI benefits and risks are in place, transparent, and implemented with accountability and full inspection. A culture of risk management must be cultivated and present.

F. Human Oversight in AI Governance: OYA must define clear structures and governance on how human oversight will be intentionally built into the adoption, review, and day-to-day implementation of AI. Clearly defined roles and responsibilities on this and the overall governance and decision-making of how, where, and when AI systems are adopted and used is critical.

G. Human-in-the-Loop (HITL): An approach in AI that ensures human input and oversight are intentionally built into the adoption, development, review, and day-to-day operation of AI systems. At OYA, HITL means that clearly defined roles and responsibilities are established in governance structures, ensuring accountability for how, where, and when AI systems are adopted and used.

H. Privacy and Confidentiality: OYA must prioritize public privacy protections in AI systems and clarify oversight responsibilities. Safety-related or emergency data use is subject to extra review.

I. Risk and Risk Management: OYA must identify, assess, measure, and manage all AI risks to ensure compliance with relevant regulations and assess projected impacts.

J. AI must not replace human judgment in decisions impacting legal rights or benefits.

K. OYA must notify youth and staff when their data is used in AI systems (e.g., AI “widgets” system integration into JJIS, Microsoft office, etc.).

L. Bias testing and equitable design must be continuous obligations, not sporadic or one-time checks.

M. Safety and Impact: AI design and use must not decrease overall safety. OYA must specify impact and safety requirements with quantifiable terms and measurement methods.

N. Security and Securing: AI system's design, use, and lifecycle management must protect it and its data from unauthorized access and must have secure and safe guardrails against alteration or destruction.

O. User Experience: AI must only be used as a tool to improve the efficiency of implementers and improve the constituent experience, not adopted as a default solution. Adoption and use of AI tools must be guided by critical consideration of the use case identified, constituent experience, and subject matter expertise within the organization.

P. Transparency and Trustworthiness: OYA must ensure clarity, openness, comprehensibility of AI processes, outcomes, impact, and decision background. All lifecycle steps of an AI system must document and share development with the public and impacted persons. Any public-facing AI outputs must include a disclosure that AI was used in their creation.

Q. Workforce Preparedness and Understanding: Staff incorporating AI systems into their workflow must be a part of the adoption discussion and be adequately informed. OYA staff must have a baseline of education in AI, covering the following areas:

1. Direct and practical application for AI;

2. Ethical considerations with AI; and

3. Privacy and data protections.

R. Mandatory Staff Training: Staff incorporating AI systems into their workflow must be required to complete training regarding AI ethics, privacy, data protection, and safe and appropriate use of AI.

V. ROLES & RESPONSIBILITIES

OYA governs AI through clear, roles-based oversight rather than a formal review board or committee. This ensures accountability today while leaving flexibility to expand as EIS guidance evolves.

A. Chief Information Officer (CIO)

1. Serves as final approval authority for all Tier 3 (High-Risk) AI use cases.

2. Approves exceptions and ensures overall policy compliance.

B. Business Owner / Program Manager

1. Defines the purpose, scope, and expected outcomes of AI use.

2. Ensures AI adoption supports OYA's mission, values, and program goals.

3. Maintains accountability for monitoring and reporting outcomes.

C. Information Security Officer (ISO)

1. Conducts risk assessments and security reviews for AI systems.

2. Ensures controls are in place to prevent data leakage, adversarial attacks, and misuse.

D. Data Steward

1. Classifies data according to OYA policy I-E-3.2 Information Asset Classification and Protection.

2. Ensures only appropriate data is used for AI purposes and that minimization practices are followed.

E. All Users

1. Must follow this policy and OYA policy 0-7.0 Use of Electronic Information Assets and Systems when using AI tools.

2. Required to complete mandatory AI training and seek supervisory guidance when in doubt about AI use.

F. Future Governance Structures

OYA must expand or formalize AI governance structures (e.g., review boards or committees) as required by future EIS statewide AI policies or directives.

VI. PROCESS

As part of AI planning and implementation, OYA must follow a formal process for identifying, documenting, reviewing, and approving AI use cases. Agency use cases and solutions must align with part IV. Guiding Principles above.

VII. DATA CLASSIFICATION & ACCEPTABLE USE

OYA complies with statewide mandates on information classification through OYA policy I-E-3.2 Information Classification and Protection. Level 3 (Restricted) and Level 4 (Critical) data are strictly prohibited from using AI tools. Attachment A: Data Classification Risk Model defines specific activities, their approval requirements and their alignment with OYA's Tier 1 -3 risk model.

Exceptions to the Data Classification Risk Model require written approval from the chief information officer (CIO) following security and risk review and may only be granted for Tier 3 AI use cases.

VIII. ENFORCEMENT

A. All OYA staff must adhere to the processes, standards, and guardrails described in this policy that ensure AI systems and tools are safe, ethical, and respect human rights. OYA must have oversight mechanisms to address risks such as bias, privacy infringement, and misuse while fostering innovation and building trust.

Violations of this policy may result in corrective or disciplinary action, up to and including dismissal from state service, in accordance with OYA and statewide Human Resources policies.

B. Staff must promptly report suspected AI misuse or AI errors impacting youth experience or outcomes to their supervisor or manager and submit an incident to the IS Service Desk for tracking and review.

Managers are responsible for assessing program impact and initiating immediate safeguards, while Information Services will coordinate technical, security, and compliance response in accordance with policy I-E-3.3 Information Security Incident Response.

IX. ETHICS REVIEW

A. High-risk AI must be reviewed by an ethics panel. OYA regularly conducts AI ethics reviews to ensure responsible development and deployment of AI technologies.

B. These reviews must address a broad range of issues including data privacy, algorithmic bias, accountability, fairness and non-discrimination, transparency and explainability, accountability, and privacy protection.

X. COMMUNITY ENGAGEMENT

Community engagement facilitates inclusion of diverse perspectives in the development and implementation of AI technologies and is a critical ingredient in creating ethical AI practices. Community engagement helps to create AI systems that are more equitable, accountable, and aligned with the populations and communities OYA serves.

A. OYA must discuss use of AI technologies with community members, system partners, and youth/family advocates when appropriate to recognize diverse perspectives, build trust, and mitigate risks associated with AI technologies.

B. Community engagement must include efforts to facilitate local discussions, build collaborative frameworks, and establish collaborative structures.

XI. TRANSPARENCY REPORTING

A. OYA’s AI processes must be open and clear as they relate to decision-making processes, algorithms, and data used in artificial intelligence systems.

B. OYA must document and share critical details about its AI systems, including the logic behind algorithms, the data used for training, and the methods for evaluation and validation.

The business owner or program manager is responsible for documenting and maintaining AI system purpose, logic, evaluation, and validation artifacts. The ISO provides required review of data sources, privacy, and security controls. The CIO ensures enterprise compliance, approval, and appropriate disclosure.

C. OYA must publish one or more reports on AI use cases, risks, and impacts annually. Disclosure documentation may take many forms, from technical documentation for regulators to simplified resources for consumers.

The CIO is responsible for ensuring annual AI transparency reporting is completed and published. Business owners and program managers provide required use case and impact content, and the (ISO) provides risk, privacy, and security disclosures.

XII. REAUTHORIZATION/SUNSETTING AI SYSTEMS

The rapidly evolving technological landscape requires agencies to make critical strategic decisions regarding which existing AI systems to maintain, which to evolve, and which to deliberately sunset as AI capabilities mature.

A. All OYA AI systems must be reviewed for re-authorization or sunsetting on a schedule established by the CIO, with input from business owners and the ISO.

B. OYA maintains a framework for identifying, evaluating, and strategically sunsetting legacy software systems while redirecting freed resources toward high-value AI investments.

D. OYA's AI review includes usage and value assessments, technical evaluations, and confirmation of strategic alignment.

XIII. LOCAL OPERATING PROTOCOL REQUIRED: NO

Attachment A: Attachment A: Data Classification Risk Model

AI Activity	Data Classification Allowed	Tier Level	Allowed	Allow with Approval	Not Allowed
Drafting internal memos, reports, or process docs for staff	Level 1-2 only	Tier 1	X		
Brainstorming ideas, summarizing meeting notes (internal)	Level 1-2 only	Tier 1	X		
Proofreading or grammar checks on non-public documents	Level 1-2 only	Tier 1	X		
Creating educational or training materials	Level 1-2 only	Tier 1	X		
Responding to public inquiries using AI-generated text	Level 1-2 only	Tier 2		Human-in-the-Loop oversight; approved disclosure text	
Generating code/scripts for internal automation	Level 1-2 only	Tier 2	X		
Generating code/scripts for systems handling Level 3-4 data	Level 3-4	Tier 3		Security review + AI-ERB approval	
Automating multi-step AI agent workflows without human oversight	Level 1-2 only	Tier 2		Pilot or sandbox only; AI-ERB review	
AI use for personal purposes on state-owned devices or networks	Any	N/A			X
Upload or share personally identifiable information (PII) – Including name, date of birth, medical records, address, contact information, case notes, and financial data for youth, staff, and stakeholders	Any	Tier 3			X
Upload or share juvenile records on any AI tools/platforms	Any	Tier 3			X
Using AI to impersonate individuals or misrepresent identity	Any	Tier 3			X
EIS specific prohibitions					
Automated public translation/transcription using AI without human review (e.g., Copilot)	N/A	Tier 3			X
Input Level 3-4 data as prompt, query, training, or to public GenAI	Level 3-4	Tier 3			X
Use GenAI without human review, assume outputs are factual, or as sole reference	Any	Tier 3			X
Use GenAI for official statements (policy, legislation, regulations)	Any	Tier 3			X