Chapter:	Agency Supports and Controls	**Effective Date: 3/9/26**
Title:	**Generative AI Usage**	Page: 1 of 3 New

(a) **Policy.**

(1) The Texas Juvenile Justice Department (TJJD) prohibits the use of unapproved generative artificial intelligence (generative AI) systems.

(2) TJJD recognizes that AI can enhance productivity, improve service delivery, and support data-driven decision-making. However, AI also introduces risks to data security, privacy, fairness, and accountability. This policy ensures that all AI use is lawful, transparent, risk-managed, and human-centered.

(b) **Applicability.**

This policy applies to all users of TJJD information technology systems or data. Users include, but are not limited to, employees, contractors, volunteers, and third parties with access to TJJD information systems and/or data.

(c) **Definitions.**

(1) **Artificial Intelligence (AI) System**--A machine-based system that infers from data to produce outputs—such as predictions, recommendations, or decisions—with varying levels of autonomy. Refers to all such systems and tools, including cloud-based systems, hybrid systems, or tools capable of creating content, such as text, images, audio, video, or code, based on patterns learned from existing data. Examples include, but are not limited to:

(A) code generation (e.g., GitHub Copilot, OpenAI Codex);

(B) content creation (e.g., OpenAI, Jasper AI, Writesonic);

(C) health care and life sciences (e.g., IBM Watson, DeepMind);

(D) image generation (e.g., Dall-E, Midjourney, Stable Fusion/Diffusion, Runway ML);

(E) music and audio generation (e.g., Amper Music, AIVA, Descript);

(F) research and data analysis (e.g., Google DeepMind, Hugging Face);

(G) agentic systems (i.e., systems that act autonomously or semi-autonomously to execute tasks or make decisions);

(H) machine learning systems (i.e., algorithms or models that learn from data to predict outcomes or recommend actions); and

(I) text-based tools (e.g., ChatGPT, Jasper, Bard).

(2) **AI Impact Assessment**--The review process evaluating legality, necessity, fairness, explainability, accessibility, and security of an AI system prior to use.

(3) **Heightened-Scrutiny AI System**--Any AI system that autonomously or substantially influences consequential decisions affecting individuals' rights, services, or benefits.

(4) **AI System Inventory**--A centralized catalog maintained by the Information Technology (IT) division and documenting all TJJD-approved AI tools, their purposes, data use, and oversight status.

(d) **General Provisions.**

(1) Staff may use only AI tools that are approved and registered in TJJD's AI System Inventory. Employees must disclose the use of AI in significant work products and cite the AI system used.

(2) Staff are prohibited from inputting confidential, sensitive, personally identifiable, or protected health information into any unapproved or public AI system.

(3) AI-generated outputs must be fact-checked and reviewed by a qualified employee prior to any dissemination. All AI use must align with TJJD ethics, branding, accessibility, and plain-language standards.

(4) The use of AI for legal research, investigations, or solicitation development, or to create deepfakes or manipulated media is prohibited.

(di) **AI Governance and Oversight.**

(1) The AI Governance Committee reviews AI impact assessments, oversees AI risk management, and coordinates with the Executive Steering Committee for strategy and prioritization. The committee comprises the chief information officer, information security officer, privacy officer, chief data officer, and other designees.

(2) The Executive Steering Committee serves as the final authority for AI policy decisions and reports annually to the executive director.

(3) Requests for AI use must include an AI impact assessment and be logged in the AI System Inventory.

(dii) **Security and Monitoring.**

The information security officer conducts vulnerability assessments, bias testing, and drift testing, and maintains audit logs of AI activity. Staff have no expectation of privacy for data used in AI systems. All AI use is subject to monitoring for compliance.

(diii) **Vendor and Third-Party Requirements.**

Vendors and third parties must comply with TJJD security and privacy standards, provide model documentation and risk assessments, refrain from using TJJD data to train models without written approval, and notify TJJD of incidents or security breaches.

(div) **Training and Awareness.**

All employees using computers for at least 25% of their duties must complete annual AI training as required by §2054.5191, Government Code. Training includes AI fundamentals, ethics, risk management, secure data handling, and bias awareness.

(dv) **Enforcement and Disciplinary Action.**

(1) Violations of this policy may result in disciplinary action, up to and including termination of employment. Contractors and third parties in violation may face termination of contracts and potential legal consequences.

(2) Users of TJJD systems or data are responsible for:

(A) adhering to this policy and refraining from unauthorized use of generative AI tools;

(B) reporting any unintentional or accidental exposure of organizational data, including using AI tools or platforms, to the IT division immediately; and

(C) obtaining approval from IT and/or the executive team prior to the solicitation or contracting of generative AI solutions.

(i) **Exemptions.**

(1) Employees may request an exemption to this policy by:

(A) completing the AI Usage Exemption Request form, IT-030; and
(B) submitting the form to their supervisor or division director.

(2) The supervisor or division director reviews the IT-030 and, if applicable, submits the form to the executive member in their chain of supervision.

(3) If approving the request, the executive member forwards it to the AI Governance Committee.

(4) The AI Governance Committee:

(A) reviews the exemption request; and
(B) forwards their recommendation and the request to the executive director or designee for final approval.

(j) **Future Policy Updates.**

This policy is reviewed annually by the chief information officer and the AI Governance Committee to ensure alignment with legislative updates and technology changes.

For additional assistance, please contact IT-Security@tjjd.texas.gov for guidance.