DRAFT

SOLANO COMMUNITY COLLEGE DISTRICT
TECHNOLOGY SERVICES PROCEDURES

GENERATIVE AI STANDARDS **PROCEDURE # 3910.13**

PURPOSE

The purpose of these standards is to guide the responsible and ethical use of Generative Artificial Intelligence (GenAI) technologies within Solano Community College District ("the District").

These tools can improve efficiency, creativity, and productivity, but they also introduce risks related to privacy, data protection, and accuracy. These standards are intended to align with the District's Information Security Program and related data protection policies.

SCOPE

These standards apply to all faculty, staff, interns, volunteers, contractors, subcontractors, consultants, service providers, and other third-parties ("users"), who use or implement GenAI tools for any institutional purpose, including administrative, instructional, operational, or communications work.

These standards apply primarily to the use of publicly accessible Generative AI systems (Public GenAI), such as ChatGPT and Gemini. The use of private AI systems developed or hosted within the District's secure IT environment must also adhere to these principles and requires IT review and approval prior to implementation.

AUTHORITY

These Generative AI Standards have been authorized and approved by the District's Information Security Officer (ISO) under the ISO's responsibility, as designated by the Board of Trustees ("the Board"), for overseeing, implementing, and enforcing the District's written Information Security Program.

EXCEPTIONS

All exceptions to this standard must be approved by the ISO.

Requests for exceptions to this standard shall be submitted, in writing, to the ISO. The request should specifically state:

- the scope of the exception along with justification for granting the exception;
- the potential impact or risk upon granting the exception;
- risk mitigation measures to be undertaken in conjunction with the exception; and

- a timeframe for achieving the minimum compliance level with the standards set forth herein.

The ISO shall review such requests and confer with the relevant stakeholders. If an exception is granted, it will be documented and reviewed at least annually.

DEFINITION OF KEY TERMS

- **Artificial Intelligence (AI):** The simulation of human intelligence by computer systems to perform tasks such as reasoning, learning, and decision-making.
- **Bias**: Unintended and systematic error in AI outcomes caused by flawed data, algorithms, or training practices.
- **Generative Artificial Intelligence (GenAI):** A type of AI that creates new content (such as text, images, or code) based on user input and learned patterns.
- **Hallucination:** A false or inaccurate response produced by an AI system that appears credible but lacks factual basis; a known limitation of large language models.
- **Large Language Model (LLM):** A machine learning model trained on large text datasets to understand and generate human-like language.
- **Machine Learning (ML):** A subset of AI in which systems improve performance over time through data-driven learning rather than explicit programming.
- **Personally Identifiable Information ("PII") –** Information that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or by which the District intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification.
    - PII includes identifiable information that is maintained in education records and includes direct identifiers, indirect identifiers, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information (see: 34 CFR 99.3).
- **Private GenAI:** Generative AI systems that are restricted and managed within the District's secure IT infrastructure.
- **Prompt:** A text input provided to an AI system to generate a response or perform a specific task.
- **Public GenAI:** Publicly accessible Generative AI systems, such as ChatGPT and Claude.
- **Sensitive Data:** Any information protected under laws such as FERPA, GLBA, HIPAA, or state privacy regulations, including personal, financial, or institutional data.

GENERATIVE AI STANDARDS

GenAI is an emerging technology, and no set of standards can cover every possible use case. As such, the following guidance is provided with the understanding that users are responsible for considering the risks of GenAI and users are accountable for all materials created or modified with AI tools.

UNDERSTANDING THE RISKS ASSOCIATED WITH GENAI

Generative AI technologies present several risks that must be considered before use in any official capacity. The following represent the primary areas of concern:

- **Sensitive Data Exposure:** Public GenAI systems often collect and retain user inputs for model improvement. Entering sensitive or regulated data, such as student, financial, personnel, or vendor information, can inadvertently expose that information outside the institution's control. Once submitted, data may be stored, processed, or reused by the provider without the knowledge of the district.
- **Data Accuracy and Hallucinations:** AI outputs may contain biases, false, outdated, or misleading information presented as fact. These "hallucinations" can introduce errors into reports, communications, or decision-making processes if not independently verified by the user.
- **Public Records and Transparency:** Prompts, outputs, and related materials generated through GenAI tools may be considered public records under the California Public Records Act (CPRA) and other government transparency legislation. Users should assume all GenAI activity could be subject to disclosure and avoid including any non-public or proprietary information in prompts or outputs.
- **Intellectual Property and Copyright:** AI-generated content may unknowingly replicate copyrighted material from its training data. Using or publishing such content without review could result in copyright violations or reputational risk to the college or district.
- **Vendor and Third-Party Risk:** Many GenAI systems are cloud-hosted by vendors outside the District's control. Use of these tools without IT review may create data handling and retention risks, including lack of transparency over data storage, deletion, or reuse.

ACCEPTABLE USE OF GENAI

Users are responsible for ensuring that GenAI use supports institutional objectives, complies with applicable laws, and adheres to professional and ethical standards.

In general, GenAI tools **may be used to:**

- Draft communications, reports, or internal documentation.
- Support brainstorming or content development.
- Summarize non-confidential materials.
- Automate routine or repetitive administrative tasks, where appropriate.

GenAI tools **must never be used to:**

- Input, generate, or process sensitive, confidential, or regulated information.
- Replace human judgment in compliance, personnel, or legal decision-making.
- Produce, distribute, or rely on unverified or misleading information.
- Signify official college communications without review and approval.

Users of GenAI **must always:**

- Verify and fact-check all AI-generated content prior to use or distribution.
- Disclose the use of GenAI tools when contributing to official publications, reports, or communications.
- Review and understand the terms of service and data handling practices for any GenAI platform prior to use.
- Opt out of data collection or model training features when such settings are available.
- Consult with Information Technology (IT) or the Information Security Officer (ISO) prior to implementing new GenAI tools or integrations into institutional systems.

Users of GenAI **must never:**

- Enter any student, personnel, financial, or other confidential institutional data into public GenAI platforms.
- Upload or share documents classified as internal, restricted, or non-public.
- Use GenAI to impersonate another individual or represent the institution without authorization.
- Rely solely on GenAI outputs to make administrative, academic, or compliance-related decisions.
- Distribute AI-generated content that could misinform, discriminate, or damage the reputation of the institution.

REVIEW OF STANDARDS

These standards shall be reviewed annually by the ISO and updated as appropriate.

CONTACT INFORMATION

All questions or concerns regarding this policy should be directed to the District's ISO.

REFERENCES

- National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework, (AI RMF 1.0).
- National Institute of Standards and Technology (NIST), Towards a Standard for Identifying and Managing Bias in Artificial Intelligence, (NIST SP 1270)
- White House Executive Order, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (Executive Order 14110).
- California Department of Technology - Information Technology (IT) Policies for Generative Artificial Intelligence (GenAI), (Technology Letter 25-01).
- Family Educational Rights and Privacy Act (FERPA), (20 U.S.C. § 1232g).
- Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, (16 C.F.R. 314.4).
- California Public Records Act (CPRA), (Cal. Gov. Code §§ 7920.000–7931.000).

AUTHORITY: Board Policy 3910

ADOPTED: <Date>