

STOCKTON UNIVERSITY



PROCEDURE

Use of Artificial Intelligence (AI) at the University

Procedure Administrator: Office of the President

Authority:

Effective Date: August 6, 2026

Index Cross-References:

Procedure File Number: 4127

Approved By: Dr. Joe Bertolino, President

I. Purpose:

This procedure provides expectations for the ethical, responsible, and secure use of all forms of Artificial Intelligence (AI) by the Stockton community at the University. It ensures that AI use supports the University's mission in teaching, research, and operations while safeguarding academic integrity, institutional, personal, and sensitive data, and compliance with all applicable laws.

II. Scope:

This procedure applies to all Stockton community members who use AI tools or systems in University-related activities, including academic work, administrative functions, and research involving University data or resources.

III. Definitions

- A. Artificial Intelligence (AI): Technologies or systems such as machine learning, natural language processing, agentic AI, Generative AI, and Large Language Models (LLM), that exhibit intelligent behavior.
 - 1. Agentic AI: A form of artificial intelligence capable of making decisions or completing tasks with minimal human oversight.
 - 2. Generative AI (GenAI): A form of artificial intelligence capable of creating new materials such as written materials, audio, video, or images.
- B. Sensitive Data: Any data protected under federal or state laws and/or institutional policy, including student records, health information, financial data, research data, and personally identifiable information (PII).
- C. Confabulation: refers to a phenomenon in which GenAI systems generate and confidently present erroneous or false content in response to prompts. Confabulations also include generated outputs that diverge from the prompts or other input, or that contradict previously generated statements in the same context. These phenomena are colloquially also referred to as "hallucinations" or "fabrications."

- D. Confidential Information: refers to any data, content, or material that is not publicly available and is protected from unauthorized access, use, or disclosure under federal or state laws and/or institutional policy. This includes, but is not limited to, PII, student records, employee records, health information, financial data, non-public research data, intellectual property, security-related information, and any third-party information provided under obligations of confidentiality.

IV. Acceptable Use of AI

A. Academic Use:

1. Faculty:

- a. Faculty may use AI to support and enhance pedagogical practices, provided the use is transparent and does not replace critical pedagogical responsibilities.
- b. In each course, all faculty should share clear expectations at the beginning of each semester through the syllabus, policy distribution, and class discussion on their expectations for the appropriate use of AI tools. Faculty may use sample AI syllabus statements provided through the University website or LMS. If permitted by the course, encourage students to acknowledge and cite any use of AI applications.
- c. Faculty are encouraged to follow best practices for disclosing the use of artificial intelligence in accordance with the standards of their academic discipline. Transparency in AI use supports academic integrity, fosters trust, and aligns with evolving expectations in research, teaching, and professional practice.

2. Students:

- a. Students should consult the syllabus for each course and understand the permissible use of AI in the course. Students should contact course instructors for clarification when needed and should seek training and support rather than risking a potential academic integrity violation.

3. Scholarly Activity:

- a. AI may be used in research with appropriate methodological rigor and ethical oversight. Disclosure of use of AI should be included in any IRB submittals.
- b. Researchers must comply with data privacy regulations when using AI to analyze human subject data or other sensitive information.

B. Administrative and Operational Use:

1. Employees may use AI tools to enhance efficiency in areas such as scheduling, communication, data analysis, and general administrative tasks, as long as the use complies with University data governance, privacy, and IT security standards.
2. Employees are responsible for reviewing and verifying the accuracy, appropriateness, and clarity of all AI-generated content prior to use or distribution. AI should support, not replace, professional judgment.
3. When the University evaluates new vendors, platforms, or technology

solutions, any embedded or optional AI functionality will be reviewed as part of the standard procurement and security assessment process. This review will determine whether the AI components appropriately align with institutional goals and ethical standards, meet University data privacy and security requirements, and support responsible, transparent, and equitable technology use.

4. Employees should consult with the IT security office when an AI tool involves sensitive data, large scale automation, system integration, or potential risk to University systems or information.

V. Statutes, Data Privacy and Security

- A. Users must not input confidential, sensitive, or personally identifiable University data into AI systems without prior approval from both General Counsel and ITS Information Security.
- B. Users must ensure self-chosen, non-university supported third party supported AI tools, comply with the University's Information Security Plan, FERPA, HIPAA, GDPR, Title II and other applicable data privacy and compliance laws.
- C. Users must not use AI tools to make decisions that significantly affect individuals (e.g., grading, hiring, student conduct) without human oversight.
- D. Users must seek guidance when in doubt. If users are uncertain whether an AI tool or use case is appropriate, or if users do not understand the requirements of this procedure, users should consult Information Security within Information Technology Services (ITS) before using the AI tool. Users should not assume a use is permissible without clarification.

VI. Ethical and Responsible Use

- A. Users must implement AI in ways that align with academic integrity, equity, and transparency.
- B. Users must check the output of AI tools for bias, inaccuracies, or confabulation.
- C. Users must follow established AI disclosure best practices that are appropriate for their specific discipline, industry standard and use case.
- D. Faculty should include clear AI-use policies in course syllabi using University recommended resources.
- E. Students are responsible for following the AI guidelines and permissible use as described in the course syllabus or specific instructions communicated to students for particular assignments, projects, research scholarly and creative activities, and other applications.

VII. Prohibited Uses

- A. Using AI to misrepresent authorship or fabricate content (e.g., research data, citations, student submissions, deep fakes).
- B. Using AI tools to generate, access, or search for dangerous or harmful content with the intent to bully, cyberbully, harass, discriminate, or cause other physical and/or emotional harm, in accordance with University Policies I-55 and I-120 and Procedures 1200 and 6940.

- C. Bypassing security controls or misusing AI to access restricted systems or data.
- D. Using AI tools to generate or search for malicious content, such as malware, viruses, etc. that may have the ability to circumvent access control measures put in place by the University, or any other third-party entity, to prevent unauthorized access to their respective networks.

E. Authorized Academic, Instructional, and Research Use

Nothing in this section is intended to restrict legitimate academic, instructional, or research activities conducted with appropriate oversight and in compliance with applicable university policies. This includes:

1) Routine, low-risk, non-decisional uses of AI for productivity (e.g., drafting emails, language editing, summarization, note-taking), unless otherwise restricted by course, school or program policies.

2) Instructional activities where AI is used for pedagogical purposes (e.g., generating synthetic or manipulated content as part of coursework), as defined by the instructor.

3) Legitimate research activities, including but not limited to the use of AI for data augmentation, synthetic data generation, or security-related research, conducted in accordance with university policies and ethical standards.

VIII. Compliance and Enforcement

- A. Violations of this procedure may result in disciplinary action in accordance with University Policy VI-13.2 and Procedure 6140. Human Resources, Academic Affairs, Student Affairs, and Information Technology Services will respectively oversee compliance, as appropriate for the alleged offense.

Review History:

	Date
Procedure Administrator	06/16/2026
Divisional Executive	06/16/2026
General Counsel	07/27/2026
Senior Leadership	08/06/2026
President	08/06/2026