SCHOOL OF VISUAL ARTS

2025 Use of Artifical Intelligence (AI) Policy

Version: 2026.03.11

Category: Acceptable Use & Communications

School of Visual Arts is hereinafter referred to as "SVA or the Institution." The Compliance Team is hereinafter consists of the Chief Information Officer, Data Privacy Officer, Chief Information Security Officer

Overview

This policy explains how AI tools and platforms may be used at the Institution and specifies what actions are prohibited. Artificial Intelligence (AI) tools, including generative and predictive systems, offer opportunities to improve teaching, learning, and operations. With these opportunities come obligations to safeguard privacy, uphold academic integrity, manage risk, and comply with accreditation requirements. While comprehensive, no policy covers every situation; users must exercise sound judgment and direct questions to their supervisor, department chair, the Office of Chief Information Officer and/or Data Privacy Officer.

Purpose

The purpose of this policy is to define acceptable use and governance of AI in support of the Institution’s mission and to ensure compliance with applicable laws and regulations, and institutional policies. Inappropriate or unmanaged use of AI tools exposes the Institution to academic, legal, operational, security, and reputational risks.

Scope

This policy applies to all users of Institutional information technology resources and data, including but not limited to students, faculty, staff, administrators, contractors, consultants, and vendors. It governs the use of any AI tool or platform (cloud-based or on premises; embedded features

or standalone services) in instruction, administration, student services, and accreditation-related activities. This policy applies to all Institutional data regardless of storage location.

Policy

4.1 Ethical Use

Use of AI must be lawful, transparent, secure, and aligned with the Institution's mission and academic standards.

AI may assist in research or create content, but staff and faculty remain responsible for accuracy, integrity, and outcomes.

Users must monitor, review, and, where necessary, correct AI generated output to avoid inaccuracies, bias, plagiarism, or misuse.

4.2 Data Privacy and Security

Do not input confidential, privileged, sensitive, regulated, or personally identifiable information (PII) into unapproved or public AI tools.

All AI use must comply with applicable privacy and security policies and requirements.

Model training on Institutional data is prohibited unless expressly approved through the vendor risk, data protection, and contract review processes through the Privacy Office.

4.3 Approved and Unvetted AI Tools

"Approved" AI tools are those evaluated and authorized by the Office of Chief Information Officer and Data Privacy Officer.

"Unvetted" AI tools may not be used with confidential, privileged, sensitive, or personal data and may not be used for official Institutional work products without authorization.

Embedded AI features in licensed enterprise software (e.g., grammar, accessibility, code assist) are permitted when the underlying product is Institution approved and data handling aligns with Institutional policy.

4.4 Procurement and Vetting of AI Tools

Departments must follow the Institution’s procurement, information security, accessibility, and legal/contract review processes prior to acquiring or enabling AI tools.

Vetting criteria include data transparency, access controls, data residency, model behavior and bias risk, content filtering, logging/audit, incident response, vendor use of sub processors, intellectual property terms, and the ability to opt out of vendor training on Institutional data.

Contracts must require Vendors to disclose use of AI in their tools and interact with SVA data and support or can impact SVA outcomes.

4.5 Vendor/Third Party Use of AI

Vendors performing services involving AI tools or platforms must comply with all applicable Institutional policies, including Information Security, Privacy, Procurement, Accessibility, and Records Retention.

Contracts must include provisions governing AI use and data handling.

Vendors must document their AI governance practices and provide transparency regarding data sources, model training, and risk mitigation.

Vendors must take reasonable efforts to notify the Institution of any significant changes to their AI systems that may affect service delivery or data integrity.

4.6 Federal, State, and Accreditation Standards

AI-generated content used in reports must be disclosed in writing at the time of submission.

The Institution is responsible for the accuracy and integrity of all submitted materials, including those generated by AI.

The Institution will not use unvetted AI tools to process confidential, privileged, sensitive, or personal information related to applicable standards.

4.7 High-Risk AI

High-risk AI tools (those impacting human rights, safety, or privacy) must undergo formal vetting and approval.

The Compliance Team must assess the bias, data quality, privacy, and security.

The Institution may prohibit deployment of high risk AI where risks cannot be mitigated to acceptable levels.

4.8 Copyright, Transparency, and Attribution

When required by policy, course, sponsor, or law, users must disclose material AI assistance and provide attribution sufficient to understand the role AI played in the work product.

Communications representing the Institution must not imply human authorship where significant AI generation occurred without required disclosure.

Users are responsible for ensuring that AI-generated materials do not infringe on the intellectual property rights of others, including copyrighted text, images, audio, or code used in prompts, training data, or outputs.

Users must not present AI-generated content as original human work for the purpose of claiming authorship, credit, or copyright protection when such claims would be inconsistent with applicable copyright law or institutional policy.

When feasible, AI-generated content should include a statement or metadata tag indicating that AI assistance was used, particularly in research, publication, or creative works intended for public dissemination.

4.9 Accessibility, Equity, and Bias

AI use must support accessibility standards. Tools should be evaluated for equitable outcomes across diverse populations, with documented mitigation where disparities are detected.

4.12 Monitoring and Privacy

AI tools in use must be re-evaluated annually for compliance.

Users should have no expectation of privacy for Institutional use of AI tools. The Institution may log, monitor, and review usage to ensure compliance with policy and law, consistent with applicable workplace and privacy policies.

Non-compliant tools must be discontinued or remediated promptly.

4.13 Training and Awareness

The institution will provide ongoing training to promote AI use and awareness of this policy.

Training will include ethical considerations, data privacy, and responsible use of AI in institutional contexts.

4.14 Prohibited Use

Inputting confidential, privileged, sensitive, or personal data into unapproved/public AI tools.

Using AI to generate or disseminate discriminatory, harassing, threatening, obscene, or otherwise unlawful content.

Circumventing security controls, attempting to deanonymize datasets, or reverse engineering models in violation of licenses.

Using AI to fabricate data, citations, research results, or credentials.

Using AI to materially mislead stakeholders or impersonate individuals.

Deploying unattended AI agents that can commit the Institution to obligations, transact, or materially alter systems without explicit authorization and safeguards.

4.15 Incident Reporting

Suspected policy violations, security incidents, data leakage, unsafe model behavior, or harmful outputs must be reported immediately to the supervisor and the Office of the Chief Information Officer and/or Data Privacy Officer and handled under the Incident Response Policy.

4.16 Exceptions

Limited exceptions may be granted by the Compliance Team or their designee.

Enforcement

This policy will be enforced by the Compliance Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of Institution property (physical or intellectual) are suspected, the Institution may report such activities to the applicable authorities.

6.0 Definitions

Artificial Intelligence (AI) : Use of machine learning, software, automations, and algorithms to perform tasks or generate predictions and content based on data or instructions.

Generative AI : AI that creates new content (e.g., text, images, audio, code, video) in response to prompts.

Predictive AI : AI that analyzes data to identify patterns and forecast outcomes.

High Risk AI : AI that may adversely affect human rights, safety, equal opportunity, access to resources, or critical infrastructure.

Approved AI Tool : An AI tool that has completed Institutional security, privacy, legal, and procurement reviews and is authorized for intended use.

Unvetted AI Tool : An AI tool that has not completed Institutional review and approval.

7.0 Revision History

This policy shall be subject to periodic review to ensure relevancy.

Date

Description of Change

Reviewer

10/28/2025

Initial Release

C. Tomescu