FEEDBACK

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

Version: DRAFT-2

NOTE: This is a clean version of the updated draft. To see the initial draft click below.

Draft-1

ADMINISTRATIVE POLICY STATEMENT

Policy Title: Responsible Use of Artificial Intelligence (AI)

APS Number: 6012 **APS Functional Area:** INFORMATION TECHNOLOGIES

Brief Description:	The University of Colorado ("University" or "CU") is committed to supporting the responsible exploration of the rapidly growing field of AI technologies while protecting privacy, ensuring security, and upholding transparency, fairness, and appropriate human oversight in alignment with its mission and values
Effective:	TBD (Pending)
Approved by:	President Todd Saliman (Pending)
Responsible University Officer:	Associate Vice President and Chief Information Officer
Responsible Office:	University Information Services
Policy Contact:	University Information Services
Supersedes:	N/A
Last Reviewed/Updated:	TBD (Pending)
Applies to:	Universitywide

Reason for Policy: Artificial Intelligence (AI), technology which enables machines to perform tasks that typically require human intelligence, has been used within higher education for many years. Recent advances in Generative AI (GenAI), a subset of AI that can create new content such as text, images, audio, video, and code, along with an emerging regulatory framework introduce novel opportunities, risks, and compliance considerations that require specific guidance. Accordingly, this Policy establishes a framework for the responsible, ethical, and secure use of AI across the University of Colorado ("University" or "CU"), with particular emphasis on GenAI.

The Policy helps ensure that AI is used in ways that protect individual rights, data, and security and advance the University's mission. It further establishes a systemwide governance framework, with focused guidance on the responsible use of GenAI across academic, research, administrative, and operational contexts at the system and campus levels.

Final decision-making authority on the use of AI at CU rests with the President and the Chancellors. This Policy ("Policy") establishes the framework within which system and campus responsibilities are defined and carried out.

I. INTRODUCTION

The use of AI for University academic, research or administrative activities ("University Activities") must comply with CU's data security, privacy, and intellectual property policies, even when such use occurs outside CU's direct visibility or control. In research or specialized contexts, separate agreements may govern AI use and should be harmonized with this Policy. University Activities include any work conducted in an official capacity on behalf of CU, including academic, research, administrative, and operational functions.

GenAI is increasingly used in teaching, learning, research, and administrative activities. At the same time, the use of GenAI introduces new and evolving ethical, legal, academic, operational, and bias-related considerations that require appropriate oversight and responsible use.

GenAI has the capability to both intake information provided by users (inputs) and to generate new or modified information (outputs). Users need to consider the security, privacy and handling of any information they provide to GenAI, as well as evaluating the quality and accuracy of the output of the system.

Unless otherwise specified, all provisions of this Policy apply to both AI and GenAI. Additional requirements specific to GenAI are identified in designated sections.

II. ETHICAL PRINCIPLES FOR AI USE

The use of AI, including GenAI, in University Activities should reflect the University's commitment to integrity, accountability, equity, and respect for individuals.

AI should be used in ways that safeguard privacy and institutional data, promote fairness and inclusion, and support appropriate and equitable access to AI capabilities, recognizing that tools and implementations may vary across disciplines and use cases. AI should also maintain appropriate security and risk management and align with the University's mission and public purpose. AI should not be used to deceive, manipulate, misrepresent or compromise the integrity of research, scholarship, or academic work.

AI should be used in ways that maintain appropriate human judgment and creativity, aligning with the University's mission to provide high-quality education and to advance research and service. Use of AI does not replace or alter existing decision-making authority. Individuals remain responsible for decisions made within their authority and must apply appropriate human oversight, accountability, and review, consistent with this Policy, proportional to the level of risk. Oversight requirements will be defined through campus AI governance processes based on risk level.

Responsibility for decisions and outcomes remains with the individual or organizational unit using AI. The University is responsible for establishing appropriate frameworks, guidance, and safeguards for the use of AI in University Activities. The University will support individuals in managing associated risks by providing institutional controls, guidance, and oversight in a manner proportionate to risk. These measures do not alter existing decision-making authority.

Transparency in the use of AI is essential to maintaining trust, accountability, and integrity in University Activities. Disclosure and explanation expectations may vary based on context, impact, and the type of AI involved. Specific disclosure requirements for Generative AI are addressed in the Responsible Use of GenAI section of this Policy.

The University recognizes that digital technologies, including AI, consume significant computational and natural resources. Consistent with CU's commitment to responsible stewardship, institutional decisions regarding AI should, where feasible, consider resource consumption and environmental impact as part of broader technology evaluation.

III. POLICY STATEMENT

A. Scope and General Requirements: This Policy governs the use of AI for University Activities by all CU students, faculty, staff, and other individuals or entities using University information technology resources or acting on behalf of the University ("Users"). All use of AI for University Activities must comply with applicable laws, regulations, and University policies and procedures. This includes, but is not limited to, laws and policies on data privacy, data governance, information technology ("IT") security, accessibility, intellectual property, and academic integrity. Key applicable CU policies and practices include:

1. Acceptable Use Policies: Users of AI must adhere to campus IT acceptable use policies which require ethical and legal use of IT resources.

2. APS 6005 – IT Security Program: CU's baseline security standards (APS 6005) apply to AI and data. Users must protect University data when using AI. Confidential and highly confidential (including but not limited to Social Security numbers, financial account numbers, driver's license/state IDs, protected health records, FERPA-protected student information or other data classified as "confidential" or "highly confidential" under APS 6010) must only be entered into AI approved for the applicable data classification. Users and departments deploying AI must ensure security controls are in place consistent with APS 6005 and do not circumvent any security requirements. Using AI does not exempt one from requirements to protect restricted data.

3. APS 6010 – Data Governance: AI that handles University data must comply with CU's data governance and data classification requirements (APS 6010). Institutional data input to or output from AI should be managed as "data assets" per APS 6010. In practice, this means data used by AI must be classified (e.g., public, confidential, or highly confidential) and protected accordingly. Data outputs from AI that are retained (such as an analysis or a decision record) become data assets and should be managed appropriately. The input of confidential and/or highly confidential data into AI that has not been reviewed and approved for use by campus IT is strictly prohibited.

4. APS 2027 Code of Conduct: AI use at CU should reflect the University's commitment to upholding the highest ethical, professional, and legal standards. AI should not be used in ways that violate conduct expectations for CU faculty, staff and students.

5. Regulatory compliance: The use of AI in decisions affecting individuals must comply with applicable federal and state laws, including the Colorado Artificial Intelligence Act. The University will provide guidance to help identify when such requirements apply and how to meet them. Data protected by law or contract must be handled appropriately when using AI.

   Users must not input, upload, or provide data to AI if doing so would violate legal, contractual, or licensing restrictions, including by enabling unauthorized access, retention, reuse, disclosure, or training by AI.

   Data subject to such restrictions may only be used with AI technologies that have been reviewed and approved for that purpose in accordance with campus governance processes and applicable data protection requirements. This includes complying with copyright restrictions when submitting content to AI systems.

   Examples of external data protection requirements include:

   a. Protected Health Information (PHI) regulated by the Health Insurance Portability and Accountability Act (HIPAA)

   b. Student information protected by the Family Educational Rights and Privacy Act (FERPA)

   c. Research data protected by conditions specified in grants and contracts which may include adherence to standards like ITAR/EAR, CMMC, FISMA, etc.

   d. Payment card data protected by contractual agreement to adhere to the Payment Card Industry Data Security Standard (PCI-DSS).

   e. Federal tax information protected by both federal and state statutes.

   f. Materials protected by United States copyright law, particularly where use may exceed permitted use or violate licensing or contractual terms.

   Not all such materials are explicitly labeled. Users are expected to apply reasonable judgment and follow institutional guidance regarding appropriate use.

   As a public institution, the University is subject to the Colorado Open Records Act (CORA). Prompts, outputs, and related records (including logs, where applicable) may be subject to disclosure upon request. The University will comply with CORA while continuing to protect information that is exempt from disclosure under applicable law, such as medical information, bona fide research records, and FERPA protected records.

6. Responsible Implementation: The approval or availability of AI for potential University use does not constitute endorsement of any specific application of that technology. University units, and individuals deploying AI remain responsible for ensuring compliance with applicable laws, regulations, and University policies and procedures.

7. Branding standards: AI-derived content used for official communications must comply with branding, communication, marketing, photography, videography, and web policies.

8. AI Model Training: University data, including information related to students, faculty, and staff, must not be used for external or commercial AI model training unless explicitly authorized through approved agreement and campus or system governance and in compliance with applicable privacy, security, and data governance policies.

9. Approved AI Technologies and Use Conditions**:** Approved AI technologies are those authorized through University or campus governance processes. Where explicitly approved, such technologies may process confidential or highly confidential University data only when appropriate safeguards, contractual protections, and security controls are in place.

   Users are responsible for adhering to published data use limitations and approved use conditions associated with the specific AI technologies and configurations. The University will maintain and communicate guidance on approved AI technologies and any applicable restrictions or conditions associated with their use.

B. Governance Structure:

The University shall establish a structure of advisory committees to inform and support leadership decisions regarding the use of AI. This structure will be rooted in existing shared governance models on each campus and at the system level.

Campus AI Committees: Each campus[1] Chancellor (or designee) shall ensure an appropriate governance structure is in place to incorporate and implement this Policy on their campus. The governance structure must include representation from campus shared governance bodies, and the Chancellor may designate a chair to provide coordination and leadership for this work. The governance structure should support coordination, guidance, and oversight related to AI use on campus, consistent with this Policy and campus governance practices.

Faculty AI Committees: Consistent with shared governance principles, faculty governance bodies are responsible for establishing and maintaining faculty-led committees or processes to address the academic and instructional use of AI, including guidance for teaching, learning, and research**.** Faculty expertise is critical to these efforts, ensuring that AI use aligns with academic standards, disciplinary norms, and pedagogical goals. These faculty-led efforts should be coordinated, as appropriate, with campus-level AI committee activities.

Systemwide AI Committee: The President shall designate a chair to convene a Systemwide AI Committee to support coordination and oversight of AI use across the University. The Systemwide AI Committee will include representation from each campus's AI governance structure, representatives from systemwide shared governance bodies, and other members as designated by the President.

The charge to the systemwide AI committee will include, but not be limited to:

- Serve as a centralized AI support and coordination body;
- Facilitate sharing of information and resources across campuses;
- Recommend common guidance (e.g., templates for AI risk assessment);
- Support consistent implementation of this Policy;
- Review and recommend AI technologies proposed for systemwide use.

The system committee should meet as needed to review the overall state of AI use at CU and recommend any updates to this Policy. Committee members are expected to serve as liaisons to their respective groups, and the chair will help ensure effective coordination and information flow across the University.

C. AI Risk Assessment: Before implementing or deploying new AI for University Activities, all University units must ensure that appropriate review and approval processes are followed consistently with campus governance structures and applicable University procedures and policies.

[1] The system administration is considered a campus for the purposes of this policy and is required to adopt any campus requirements herein.

AI used in decisions affecting individuals (such as employment, admissions, financial determinations, or disciplinary actions) must be applied with appropriate human judgment and oversight.

AI use cases that present elevated risk, such as those that significantly shape or determine outcomes for individuals, must be reviewed through campus AI governance processes prior to deployment, consistent with applicable federal and state laws.

AI that may process University data, significantly shape decisions affecting individuals, or be integrated with University systems must undergo appropriate review prior to use. Such review may include evaluation of:

- Data privacy and data classification requirements
- Information security controls and compliance with APS 6005
- Data governance requirements under APS 6010
- Accessibility requirements under applicable laws and University policy
- Legal and contractual obligations
- Potential risks related to bias, fairness, or unintended effects on individuals
- Effects on existing content, data, technology and business processes
- Fiscal and other resource requirements

Campus AI governance committees may recommend risk assessment frameworks or review processes appropriate to the level of risk associated with the AI technology.

For example, AI use cases may be evaluated based on risk, including but not limited to:

- Low risk: minimal impact, no confidential data, no decisions affecting individuals
- Moderate risk: involves institutional data or internal processes or professional activities
- High risk: involves highly confidential data, automated or assisted decisions affecting individuals, including those made in administrative, academic, or professional contexts, or has significant institutional impact

These categories apply to both centralized systems and individual or unit-based use cases. Higher-risk uses require more rigorous review, documentation, and oversight through campus governance processes.

D. Responsible Use of GenAI: GenAI, as a subset of AI, is governed by the scope and general requirements set forth earlier in this policy. Consistent with those provisions, the University of Colorado commits to a transparent and appropriate human-centered approach to GenAI. To that end:

1. Disclosure of GenAI Involvement: Users should be transparent about the use of GenAI when it contributes to University decisions or other high-impact outputs created in an official University capacity, considering the context and potential impact. When GenAI substantially shapes content, analysis, or decisions, users should be prepared to explain, at a reasonable level, how GenAI was used, consistent with available tools and institutional guidance.

   Routine or incidental uses of GenAI for drafting, editing, formatting, or similar assistive purposes (e.g., spell check, grammar suggestions, or rewriting tools) do not require disclosure.

   Specific contexts, including coursework, research, and administrative functions, may require more detailed or stringent expectations regarding the disclosure and use of GenAI. These expectations will be communicated through established channels appropriate to each context. Users are responsible for adhering to applicable requirements established by instructors, academic units, research sponsors, or administrative authorities.

2. Human Oversight and accountability: All members of the CU community are accountable for the work they produce, regardless of the level of GenAI involvement. The use of GenAI outputs should always involve human oversight that is proportional to the effects of the use of GenAI on the CU community. For example, using GenAI to create an image for a poster may need a simple visual inspection, whereas the use of GenAI in the creation of legally binding documents may need detailed review by trained professionals. GenAI can create content with notable errors and flaws, making the review of outputs a critical step in the responsible use of GenAI. GenAI is intended to support, not replace, human judgment. Individuals using GenAI, including outputs produced through

embedded or automated GenAI features, are responsible for ensuring their accuracy and appropriateness. Use of GenAI for fraudulent, deceptive, or harmful purposes is inconsistent with university policy and may be addressed under applicable university conduct policies.

3. Use of GenAI in CU coursework: This APS establishes baseline expectations for the responsible use of GenAI in coursework. Campuses may provide additional guidance on acceptable academic uses of GenAI consistent with this APS.

   Schools, colleges, departments, or academic programs, through appropriate shared governance processes, may also establish guidance regarding the use of GenAI in coursework or instructional activities within their academic units. Such guidance must be consistent with this APS and applicable campus policies and procedures. Within these parameters, instructors establish expectations and guidelines for GenAI use in their courses, and students are responsible for adhering to those expectations.

   A student's failure to adhere to instructor expectations regarding the use of GenAI may result in consequences determined through course and campus academic integrity processes.

4. Use of GenAI in research and academic works: The use of GenAI in the course of research and the creation of academic works must adhere to any requirements specified for the intended use. This includes adhering to any GenAI usage rules from academic journals, conferences, and sponsoring organizations.

5. Use of GenAI in administrative and staff work: University staff may use GenAI to support administrative, operational, and service functions, provided such use complies with this policy and other applicable University policies and procedures regarding data privacy, information security, and records management. Staff are responsible for ensuring that:

   - Confidential or highly confidential University data is not entered into GenAI unless the technology has been reviewed and approved for such use by the University.
   - Outputs generated by GenAI are reviewed by the user for accuracy by the user, bias, and appropriateness before being used in official University business, with the level of review proportional to the context and potential impact.
   - GenAI is used to assist, not replace, professional judgment, institutional responsibilities, or required approvals.

   Supervisors and units may establish additional guidance for the appropriate use of GenAI in administrative functions, consistent with this policy and in coordination with campus and systemwide guidance where appropriate.

6. GenAI depiction of real people: GenAI representations (images, video or voice) of real people must not be created or distributed without their explicit, informed consent, unless the use is part of:

   - Coursework by students under faculty supervision that depicts public or historical figures solely for educational purposes and is created within the faculty member's guidelines for the use of GenAI, and in furtherance of learning with no intent to deceive or cause harm. For example, a student in a history course includes a GenAI generated depiction of a former president of the United States as part of an assignment that permits the use of GenAI generated components.
   - Faculty-created educational content that depicts public or historical figures for instructional clarity, satire, or social commentary, provided the context is clearly communicated and there is no intent to deceive or cause harm. For example, a faculty member creating a visual guide to the physics topic of special relativity that includes a GenAI generated depiction of Albert Einstein.

   These expectations also apply to university-created, public-facing content, including communications, marketing, and promotional materials, particularly where AI is used to generate or modify depictions of real individuals.

In all cases, GenAI depictions of real people must include sufficient context or disclosure to avoid material misrepresentation or confusion about whether the depiction is authentic.

7. GenAI depictions of people in official CU communications and marketing: Notwithstanding the exceptions described in III.D.6, GenAI must not be used for realistic depictions of people in official CU communications and marketing materials.

8. Creation of sexualized content using GenAI: GenAI technologies must not be used to create sexualized content depicting real individuals without their explicit, informed consent.

E. Violations: Policy violations may result in disciplinary action consistent with applicable University policies and procedures, including but not limited to employee discipline, student conduct processes, termination of access to University systems, and other administrative or legal remedies as appropriate.

IV. RELATED POLICIES

A. APS 5065 - Protected Class Non-Discrimination
B. APS 6005 - IT Security Program
C. APS 6010 – Data Governance
D. APS 2027 – Code of Conduct
E. Campus IT Acceptable Use Policies
F. Colorado Consumer Protection Act on Artificial Intelligence (C.R.S. 6-1-1701 - 6-1-1707)

V. HISTORY

Review Cycle**:** This Policy will be reviewed on a periodic basis and more frequently as needed to address changes in technology, applicable law, and University practices.

- Adopted: TBD (Pending)
- Revised: N/A
- Last Reviewed: TBD (Pending)