



APPROVED BY THE BOARD ON 6/20/2026

TECHNOLOGY & ARTIFICIAL INTELLIGENCE (AI) USE POLICY

written by Stephanie Valadez, President & Andrew Martin, UC Merced EVP

Spring 2026

Adopted by the Board of Directors on 6/20/2025

PURPOSE

As the University of California continues to explore innovative uses of technology across individual campuses and systemwide, a number of concerns must be broached in order to maintain the integrity, institutional autonomy, and calibre of work that is a hallmark of the UC system. UCGPC seeks to develop and instill a series of *Guiding Principles* to facilitate the building of a UC 'Trusted AI Standard'. This policy brief is the first step in UCGPC's support of innovation and productivity, while protecting privacy, academic integrity, intellectual property, values, and the environment.

SCOPE

Policy guidelines discussed apply to a broad set of technologies including:

- Generative AI used for organizational work (ie. Text, images, code generation, etc.)
- Predictive analytics
- Digital infrastructure and institutional platforms
- Digital sovereignty in the pursuit of university autonomy

Examples include but are not limited to:

- AI based writing assistants
- AI Image generators
- Research and data-analysis tools
- Surveillance technologies
- Digital Infrastructure Involved in Graduate Student Work

BACKGROUND

UCGPC seeks to avoid tech doomerism and utopianism by opting for a pragmatic approach to the use of technology and AI. New technologies may reduce costs and create new efficiencies, but UCGPC must remain conscious of the inequities that emerge from the use of technologies within higher education. Private surveillance services, such as Flock, are prone to data hacks, biased policing, and

discriminatory searches leading to costly lawsuits for cities¹. The recent hacking of online education tools such as Canvas exposed student information, disrupting the university's teaching abilities during finals. Finally, political attacks on universities suggest creating easy to access student data systems can be to the detriment of graduate students, especially international, undocumented, and politically active students exercising their legal rights. These and other instances demonstrate how technologies integrated into campus infrastructure produce exploitations that harm stakeholders across the UC.

Definitions and Backgrounds of Key Pillars of New Technologies

Given the breadth of new technologies emerging, it is helpful to provide definitions and background on key terms. This list is not exhaustive, rather an attempt at building a language to discuss technologies that policy guidelines apply to.

Artificial Intelligence (AI)

A broad set of technologies often based on large language models (LLM's) that are used to automate a variety of tasks including decision making, classifying, making recommendations, transcribing or translating, and text and image generation. It is important to remember that AI is largely a marketing term and does not specify what a technology is or does². When AI is used in this document it is referencing a larger set of individual technologies that can possess both shared and unique characteristics and concerns.

Sensitive Data

Technology firms increasingly collect large amounts of personal data when providing access to technologies and services. Personal data ranges from facial recognition, passwords, financial information, medical history, and more. Data is generated through interactions with technology products and services through monitoring, which is then packaged and either used to refine products, sold to data brokers, or provided to the government³. The variety of services universities provide make them prime locations for the production, packaging, and transferring of data.

Sensitive data exists through specific data points, such as social security numbers. Data can also become sensitive when aggregated through a collection of different points that produce user profiles. Tech firms increasingly offer free or discount services and products in exchange for

¹ Hamid, Sarah. 2025. *EFF's Investigations Expose Flock Safety's Surveillance Abuses: 2025 In Review*. Electronic Frontier Foundation.

² Bender, Emily M. and Hanna, Alex. *The AI Con*. 2025. Harper.

³ Lamdan, Sarah. 2023. *Data Cartels: The Companies That Control and Monopolize Our Information*. De Gruyter eBook-Paket Rechtswissenschaften. Stanford, California: Stanford University Press.

access to user data. The result is the blurring of the line between valuable data on the one hand and sensitive data on the other, both of which are increasingly out of the hands of users and universities.

Digital Sovereignty:

Digital sovereignty originates as a project undertaken by cities seeking to maintain their autonomy when forming partnerships with stakeholders from a broad range of groups including private tech firms, venture capital, communities, workers, and local, state, and federal governments⁴. Digital sovereignty is the ability of organizations to develop, implement, monitor, and change independent policies based on criteria internal to the organization.

For the University of California, the task of digital sovereignty rests on maintaining the autonomy of the institution across three key operations that exist system wide and within individual campuses: research, teaching, and administrative operations. While these areas possess distinct characteristics and processes, they are also interrelated, with digital infrastructure and technology shaping what is possible and what outcomes are achieved.

UCGPC's guidelines seek to foster and protect the autonomy of the UC through policies that prioritize digital sovereignty.

GUIDING PRINCIPLES

Building out of UCOP's framework for system wide consideration of AI, UCGPC positions its guiding principles into four keystones: (i) *Interdisciplinary Solutions to Grand Challenges*, (ii) *AI in Health*, (iii) *UC's Development of a Trusted AI Standard*, and (iv) *Infrastructure and Computing*.

Guiding principles within each keystone are not taken as independent from one another, rather can interlock with one another and play a role informing strategies for how to address opportunities and challenges. UCGPC's *Guiding Principles* are spread across 10 domains.

- *Environmental Concerns*
- *Equity & Non-Discriminatory*
- *Human Oversight*
- *Transparency*
- *Accuracy & Reliability*
- *Security*

⁴ Morozov, Evgeny, and Francesca Bria. n.d. "Rethinking the Smart City: Democratizing Urban Technology". 2018. Rosa Luxemborg Stiftung. New York Office. New York, NY.

- *Privacy & Data Protection*
- *Policy Review*
- *Compliance*
- *Intellectual Property & Copyright*

UCGPC will develop a roadmap on these issues with regards to each of the UCOP AI Steering Committee's Opportunity Areas. This will provide a comprehensive series of leverage points that the UC can develop in its pursuit of a 'Trusted AI Standard'.

We expect that members of our organization will adhere to the following guidelines:

1. Environmental Concerns

- UCGPC recognizes that AI technologies require substantial computational resources, energy and water consumption, and infrastructure capacity. Universities are encouraged to consider the environmental impact of AI systems and to use these tools responsibly and efficiently.
- Use of these technologies should be used judiciously to minimize unnecessary waste of resources.
- UCGPC supports ongoing evaluation of emerging best practices to guide the future of AI to move sustainable and environmentally conscious practices.

2. Human Oversight

- AI systems must only be used to support, not replace human labor, accountability, and decision-making. Responsibility for all decisions and output produced remain with the individual using the technology.

3. Accuracy and Reliability

- AI-generated content often contains fabricated or misleading "hallucinations" therefore must not be relied on without review.
- Users must verify all AI-generated output, specifically for:
 - Accuracy
 - Bias
 - Completeness

4. Privacy and Data Protection

- Users may not input confidential, restricted, protected, or personal information into public/open AI systems.
- Protected Data includes:

- Student records
- Financial records
- Health information
- Research data
- Or any other personally identifiable information.

5. Equity and Non-Discriminatory Practices

- AI systems must not be used in ways that discriminate against individuals or groups based on race, gender, (dis)ability, religion, national origin, sexual orientation or any other similar categories.
- See UCGPC's [Anti-Discrimination and Anti-Harassment Policy](#)

6. Transparency

- AI-generated material must never be presented as entirely human-created work when disclosure is required, including the following situations:
 - University of California Guidelines
 - Research protocols
 - Publication standards
 - When requested by the UCGPC Board of Directors

7. Security

- No confidential UCGPC materials or student data should be shared with unrestricted AI tools
- No personal data or student data should be shared with unrestricted AI tools.

8. Intellectual Property and Copyright

- No copyrighted material or intellectual property of which you are not the owner should be input into AI tools without the explicit written consent of the owner.

9. Compliance

- Acceptable Uses (with appropriate disclosures)
 - Brainstorming
 - Drafting and editing assistance
 - Data Analysis
 - Accessibility accommodations
 - Administrative efficiency with full consent of all parties present

- Prohibited Uses
 - Uploading sensitive or confidential information
 - Plagiarism or academic dishonesty
 - Harassment, discrimination, or creating harmful content
 - Deepfake or impersonation activities
 - Decision-making without human oversight
 - Misrepresenting AI content as entirely human-created work

11. Violation of this policy may result in:

- Internal discipline
- Sanction
- Legal action
- Serious violations involving privacy breach, fraud, or misconduct may be escalated to the appropriate authorities.

10. Policy Review

- This policy must be reviewed semi-annually to address the following:
 - Technological advances
 - Regulatory changes
 - Evolving best practices

Questions or concerns regarding AI use or this policy should be directed to the UCGPC Secretary.

Approval:



- Secretary:

Ramiro Cabanillas-Ledesma

Date: 6/20/26