# Guidance on Data Privacy and Security When Using AI Tools in Instruction

Instructional Technology & AI Committee

## Purpose

These guidelines explain how existing Santa Monica College Board Policies and Administrative Regulations related to student records, privacy, and acceptable technology use apply when faculty use artificial intelligence (AI) tools in instructional contexts.

The purpose of this document is to:

- Clarify what existing SMC policy and federal law (FERPA) require when AI tools are used in instruction
- Provide a practical data classification system to help faculty make quick, informed decisions about what information is safe to input into AI tools
- Distinguish between consumer AI tools and institutionally approved AI tools, and explain why the difference matters
- Offer a step-by-step decision process and quick-reference guide for everyday use

These guidelines do not create new requirements and do not supersede Board Policy or Administrative Regulation. Based on SMC policies, this document is not a requirement and is not intended to replace any existing policies related to student privacy or data security.

*Core Principle: Treat every AI tool the same way you would treat handing a document to a stranger. If you would not hand that person a document containing a student's name, grades, or personal information, do not enter that information into an AI tool.*

## Policy Framework

Faculty use of AI tools is governed by existing District policies, including:

- Administrative Regulations on Student Records and FERPA Compliance (AR 5040 / AR 5040.1, Chapter 5 — Student Services)
- Board Policies and Administrative Regulations governing appropriate use of District technology resources (AR 3720)
- Districtwide obligations to protect student education records and personally identifiable information (PII)

DRAFT

Santa Monica College complies with the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records in any format, including electronic and digital records. Under AR 5040 and AR 5040.1, student education records include any recorded information that is directly related to a student and is maintained by the College or by a party acting on behalf of the College.

*Key Implication: Using an AI tool does not exempt faculty from FERPA obligations. AI tools operated by third parties are treated as external recipients of information unless formally contracted and authorized by the District.*

## What FERPA Prohibits

Based on AR 5040 / AR 5040.1, faculty must **not disclose or input** into AI tools:

- Student names, student ID numbers, grades, evaluative feedback, enrollment status, or academic standing
- Any information that identifies a specific student's academic performance or educational history
- Student assignment submissions, writing samples, discussion posts, or advising notes — whether graded or ungraded (once submitted to an institutional system such as Canvas, these meet FERPA's definition of education records)
- Education records protected under FERPA, whether draft or final
- Confidential institutional records not intended for public disclosure

FERPA permits disclosure of education records only with student consent or under a defined FERPA exception (e.g., school officials with legitimate educational interest). AI vendors and publicly available AI tools do not qualify as school officials unless the District has entered into a formal contractual relationship that meets FERPA requirements.

## Data Classification Levels

The following four-level system helps faculty make quick, clear decisions about what information is appropriate to input into an AI tool. Levels are based on the harm that would result if the data were exposed.

**LEVEL 1 — PUBLIC DATA** Safe for any AI tool

DRAFT

Information that is already publicly available or was created for public use. No harm would result from its disclosure.

- Published course catalog descriptions, publicly posted syllabi
- General college information (campus address, department contacts, office hours)
- Publicly available academic content (textbook passages, published articles, open educational resources)
- Your own original instructional materials that contain no student-identifiable data
- Generic, de-identified teaching scenarios ("A student asks about the quadratic formula")

**LEVEL 2 — INTERNAL DATA** Use ONLY with institutionally approved AI tools

Information not intended for public release but not legally protected. Disclosure would cause moderate institutional harm.

- Internal college memos, meeting notes, committee documents not publicly posted
- Draft policies, internal planning documents, budget discussions
- Unpublished course materials you do not intend to share publicly
- De-identified, aggregated student outcome data (e.g., "78% of students passed this assignment" with no individual identification)

**LEVEL 3 — SENSITIVE DATA** Use ONLY with enterprise-licensed, FERPA-compliant AI tools

Data protected by law (FERPA, CCPA/CPRA) or by institutional policy. Unauthorized disclosure would cause significant harm.

- Student names combined with grades, enrollment status, or academic performance
- Student assignment submissions, whether graded or ungraded (once submitted to an institutional system, these are education records under FERPA)
- Advising notes, financial aid data, accommodation records
- Class rosters with student IDs
- Faculty personnel records, performance evaluations

**LEVEL 4 — RESTRICTED DATA** NEVER input into ANY AI tool

DRAFT

Data whose exposure would cause severe harm, legal liability, or identity theft. No AI tool — including enterprise-licensed ones — should be used with this data without explicit institutional approval from IT security.

- Social Security Numbers, driver's license numbers, passport numbers
- Bank account or credit card numbers
- Medical or health records (HIPAA-protected information)
- Passwords, security credentials, authentication tokens
- Legal case files, active litigation documents

*Note: A list of AI tools approved for use with Level 2 and Level 3 data is under development by the institution and will be published when available. Until that list is finalized, faculty should consult IT or the Instructional Technology & AI Committee before using any AI tool with Level 2 or Level 3 data.*

---

# Consumer Tools vs. Institutionally Approved Tools

The version of an AI tool you use matters for data privacy. A free, consumer account and an institutionally licensed account may use the same underlying AI model but have fundamentally different data handling practices.

## Consumer (Free/Personal) AI Tools

When you use a free AI tool with a personal account, you are typically agreeing to terms of service that allow the company to store your inputs, use them to train their models, share data with third parties, and retain your data indefinitely. Consumer tools should only be used with Level 1 (public) data.

## Institutionally Approved AI Tools

When the college provides an AI tool through an institutional license — authenticated with your college credentials — the institution has typically negotiated contractual protections that prohibit the vendor from using your inputs for model training, require FERPA-compliant data handling, and subject the vendor to institutional security reviews.

### What Is Currently Available to SMC Faculty?

As of early 2026, the following AI tools are available to SMC faculty through institutional or systemwide partnerships:

DRAFT

- *Google Gemini for Education and NotebookLM* — Available to all California community college faculty through the CCCCO/Google partnership. Enterprise-grade data protection; data is not used to train AI models. Authenticate with your institutional Google Workspace account.
- *Microsoft Copilot* — Available through SMC's Microsoft 365 deployment. When logged in with your institutional account, Copilot provides enhanced data protections. Verify with IT whether Copilot features are enabled for your account.
- *Adobe AI features* — Available through SMC's Adobe institutional license. Use with your college credentials for institutional data protections.

Additionally, the following AI tools are in use for instructional purposes at SMC. These tools have been vetted by the California Community Colleges Chancellor's Office but have not yet been reviewed by SMC's IT Department:

- *Nectir AI*
- *PlayLab AI*

*Important: Always use the institutionally provided version of an AI tool when one is available. The same AI model accessed through your college's licensed platform has fundamentally different privacy protections than the same model accessed through a free personal account. SSO (single sign-on) integration alone does not mean a tool has been approved for use with sensitive data.*

---

# Before You Use an AI Tool: A Decision Process

Use this process every time you consider entering information into an AI tool. With practice, these decisions will become second nature.

## Step 1: Identify the Data

Before you type anything, ask: What information am I about to enter? Does it contain any student names, IDs, grades, assignment text, or personal details? Does it contain confidential institutional information?

## Step 2: Classify the Data

Use the four-level system (above).

- Level 1 (Public) → proceed with any tool.

DRAFT

- Level 2 (Internal) → use only an institutionally approved tool.
- Level 3 (Sensitive) → use only an institutionally approved, FERPA-compliant approved tool and consider whether you can accomplish the task without entering the sensitive data at all.
- Level 4 (Restricted) → do not input into any AI tool.

### Step 3: Choose the Right Tool

If your data is Level 1, you may use any AI tool. If your data is Level 2 or 3, use only an institutionally approved tool and authenticate with your college credentials.

### Step 4: Minimize the Data

Even when using an approved tool, enter only the minimum data necessary. In most instructional use cases, you can describe a situation generically instead of entering actual student data. Instead of "My student John failed the midterm," try "A student in an introductory biology course failed the midterm. What are effective intervention strategies?"

### Step 5: Verify the Output

After using the AI tool, review the output for accuracy. AI tools produce errors, fabricated citations, and biased content regularly. Do not use AI output without verification.

*The Simplest Rule - If you are unsure whether the data you are about to enter is safe, do not enter it. Ask the Instructional Technology & AI Committee, your department chair, or SMC's IT Department. There is no penalty for asking; there can be significant consequences for guessing wrong.*

---

## Quick Reference

**You CAN:**

- Use any AI tool to brainstorm lesson plans, generate rubrics, create quiz questions, or draft instructional materials — as long as you do not include student-identifiable data
- Use an institutionally approved AI tool to work with internal college documents that do not contain student PII
- Ask AI tools for general pedagogical advice ("What are effective strategies for teaching statistical inference to community college students?")

DRAFT

- Use AI to assist with your own professional writing (committee reports, grant narratives, letters of recommendation drafted generically first and personalized offline)
- Direct students to use institutionally provided AI tools for course activities you have designed

**You CANNOT:**

- Enter student names paired with grades, IDs, or performance data into any AI tool (even approved ones, unless specifically authorized by IT for that purpose)
- Copy student assignment submissions into a consumer AI tool for grading or analysis
- Upload class rosters, grade sheets, or advising records into any AI tool
- Enter Social Security Numbers, medical records, financial account numbers, or passwords into any AI tool under any circumstances
- Require students to create accounts on AI platforms that have not been vetted by the institution for data privacy and accessibility
- Assume that a consumer (free) AI tool has the same privacy protections as an institutionally licensed one

---

## Frequently Asked Questions

**Q: Can I paste a student's essay into ChatGPT to help me write feedback?**

No. A student's assignment submission — whether graded or ungraded — is an education record under FERPA once it has been submitted to an institutional system like Canvas. Pasting it into a consumer AI tool constitutes disclosure to a third party without consent. Instead, describe the issue generically: "Write constructive feedback for a college student whose argumentative essay has a strong thesis but weak evidence."

**Q: Can I use AI to generate a rubric or quiz questions?**

Yes. Creating instructional materials with AI is a Level 1 use, as long as no student-identifiable data is included in your prompts. This is true for any AI tool.

**Q: What about running student work through an AI detection tool like GPTZero?**

This requires careful analysis. A student assignment submitted through Canvas is an education record under FERPA regardless of whether it has been graded — the "maintained

DRAFT

by the institution" criterion is met the moment the work enters the LMS. Submitting that record to a third-party detection service that has no data use agreement with the college may constitute an unauthorized FERPA disclosure. If you choose to use a detection tool, you must at minimum remove all personally identifiable information before submitting (see the next question for what that requires). Beyond FERPA, faculty should also be aware that AI detection tools have documented accuracy limitations, including higher false-positive rates for non-native English speakers. The Instructional Technology & AI Committee recommends consulting with IT before using any third-party detection service.

**Q: If I remove a student's name from their work before submitting it to a detection tool or AI service, does that resolve the FERPA issue?**

It depends on how thoroughly the work has been de-identified. Under FERPA, data is considered de-identified only when all personally identifiable information has been removed — including any information that, alone or in combination, would allow a reasonable person in the school community to identify the student with reasonable certainty. Removing a name from a generic analytical essay may be sufficient. But a personal narrative containing unique biographical details — a specific immigration story, a particular family circumstance, a description of a disability — could still identify the student even without a name attached. FERPA's "reasonable person" standard asks: could someone in the campus community who reads this content figure out who wrote it? If the answer is possibly yes, the work has not been adequately de-identified. When in doubt, do not submit the work to a third-party tool.

**Q: I use my college Google account for Gemini. Is that the same as using Gemini for Education?**

Yes — if you are logged in with your SMC institutional Google Workspace account, you are accessing Gemini under the CCCCO/Google partnership with enterprise-grade protections. If you are logged in with a personal Gmail account, you are using the consumer version with no institutional protections. The account you are logged into is what matters.

**Q: Can I upload a class roster to an AI tool to create a seating chart?**

No. A class roster contains student names paired with enrollment data, both of which are protected under FERPA. Use institutional systems like your SIS (e.g., mProfessor/WebISIS) or Canvas for tasks that require roster data.

**Q: I want to use an AI tool that's not on the approved list. What do I do?**

DRAFT

Contact the SMC Information Technology Department to request a review. Do not assume that a tool is approved because your department has purchased it or because it supports single sign-on. A formal review is required before any AI tool can be used with Level 2 or Level 3 data.

**Q: Once I enter data into an AI tool, can I delete it?**

In most cases, no. It is extremely difficult — and in many cases impossible — to remove data once it has been entered into an AI system. This is one reason prevention is critical: the safest approach is to never enter protected data in the first place.

**Q: Does the California Consumer Privacy Act (CCPA/CPRA) apply here too?**

Yes. California's privacy laws provide additional protections beyond FERPA, including students' right to know what data is collected and the right to request deletion. AI tool providers that process student personal information may be subject to these requirements. FERPA is the primary framework for education records, but CCPA/CPRA reinforces the importance of limiting data disclosure to third parties.

**Q: Does AB 2370 affect how I use AI in my courses?**

AB 2370 prohibits AI from replacing community college faculty for providing academic instruction. While it is primarily about instructional authority rather than data privacy, it reinforces the principle that AI tools operate under faculty oversight and within institutional governance — not independently. (Add context from AB 2370)

---

# Resources

**SMC Policy References**

SMC Board Policy Manual (including AR 5040, AR 5040.1, AR 3720)

https://admin.smc.edu/administration/governance/board-of-trustees/board-policy-manual.php

SMC FERPA Information

https://www.smc.edu/admission-aid/student-records/ferpa.php

SMC Instructional Technology & AI Committee

https://admin.smc.edu/administration/governance/academic-senate/committees/instructional-technology-ai.php

**Federal and State Law**

DRAFT

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g

https://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)

https://oag.ca.gov/privacy/ccpa

California Assembly Bill 2370 (AB 2370)

https://legiscan.com/CA/text/AB2370/id/2925441

**California Community College Sources**

ASCCC (2024). Academic Integrity in an AI World: Resource Document

https://www.asccc.org/sites/default/files/ASCCC_AI_Resources_2024.pdf

CCCCO & Google (2025). California Community Colleges and Google AI Partnership

https://www.cccco.edu/About-Us/News-and-Media/Press-Releases/2025-ai-partnership-with-google

CCCCO (2025). Vision 2030 Artificial Intelligence Workplan

https://www.cccco.edu/-/media/CCCCO-Website/docs/vision2030/artificial-intelligence-workplan.pdf

## Revisiting These Guidelines

AI tools and the policies governing their use are evolving rapidly. These guidelines will be reviewed and updated periodically by the Instructional Technology & AI Committee as technology, institutional policy, and legal requirements change.

Faculty are encouraged to share feedback on these guidelines with the Instructional Technology & AI Committee at any time.

DRAFT