

What Can I Put Into an AI Tool as a Faculty Member

CU Faculty Council AI Committee | Guidance for Faculty | AY 2026–27 *This document offers guidance on [APS 6012](#), [CU Data Classification](#), and the [Student Data Use Guidelines](#). It is advisory and does not create policy.*

In practice: Entering confidential or highly confidential material into an AI tool that campus IT has not reviewed and approved for that classification is prohibited (APS 6012, III.A.3). Faculty are responsible *both* for what they **put into any** generative AI tool (III.A.2–3, 8) **AND** for **disclosing** AI use when it contributes to University decisions or other high-impact outputs created in an official University capacity (III.D.1).

What this means for your work

- **Grades and student work that will be graded are confidential data.** Pasting a set of submissions or other material intended for a grade or formal evaluation into an unapproved chatbot or other GenAI tool is prohibited unless that tool is approved for confidential data.
- **An accommodation letter is more sensitive than a grade.** Disability information sits a full tier above grades. Accommodation correspondence, and anything revealing a student's disability, requires a tool approved for highly confidential data.
- **Directory information is the only public student data.** Although students may suppress directory release under FERPA.
- **Removing the name does not declassify it.** A paper is often identifiable from its content.
- **Students have intellectual property rights.** Students retain ownership of their original work (III.A.5.b), and University data must not feed external model training without affirmative and informed consent from all intellectual property owners (III.A.12).
- **Your own research may be confidential data, too.** Per CU's Data Classification Table (below), research proposals and plans are confidential along with internal memos and work-related emails.
- **Third-party ownership and intellectual property rights must also be considered.** *Data subject to third-party ownership or intellectual property rights must not be used for any AI model training without affirmative and informed consent by all intellectual property owners (III.A.12).*

Brief Recommendations on Best Practices (coming soon)

Student material, specifically (see descriptions of tiers/levels below)

Faculty Activity	Security Level	Tool Classification Level	Output impact and disclosure
Draft feedback on a submitted assignment that will be graded or an activity that will be formally evaluated	Student work — level 3	Confidential	High. Contributes to a grade; disclose.
Provide feedback that is not tied to a grade or formal evaluation	Student work—level 2	Confidential	Low. Disclosure not required.

Score, rank, or compare a set of submissions	Student work and grades — levels 2–3	Confidential	High. Disclose. (III.D.2).
Summarize class performance, GPA, or progress toward continuation	GPA, probation, suspension — level 3	Confidential	High where it informs continuation or standing.
Draft a letter of recommendation or a program evaluation	Grades and record data — levels 2–3	Confidential	High. Significantly affects an individual; disclose.
Work with an accommodation letter, or anything revealing disability, race, citizenship, visa status, or religion	Level 4	Highly confidential	High. The stricter input rule applies whatever the output.
Check suspected unauthorized AI use in student work	Student work — level 2	Confidential	High. Informs an allegation; a detector score is not a finding.
Draft a rubric, assignment prompt, or syllabus language	No student data	Any tool permitted for the material	Low. No disclosure required under III.D.1.
Use only directory information, such as a name or enrollment	Level 1	Any tool	Low. Suppressed directory data is not public.

CU Data Classification Table

Type	Description	Examples
Highly Confidential	This type includes data elements that require protection under laws, regulations, contracts, relevant legal agreements and/or require the university to provide notification of unauthorized disclosure/security incidents to affected individuals, government agencies or media. Requirements when accessing, handling or storing: When possible, use university-supported services or systems that have been approved for handling highly confidential data.	- Protected health data - Social Security numbers - Payment card numbers - Financial account numbers including university account numbers, student account numbers and faculty and staff direct deposit numbers - Driver's license numbers

	• Only share with the people who are authorized to use it for legitimate business purposes; this includes verbal and written information. • Encrypt the data when sending or storing. • Ensure networks or systems used to handle or store the data have appropriate firewalls, monitoring, logging, patching, anti-malware, and related security controls. • Use university-provided computers when accessing or processing data. If this is not possible and you must use a personal computer, use a remote desktop to connect to your university-provided computer. • Document the policy for data retention. • Contact your campus information security office to ensure protection of data if compensating controls are used to secure the data in place of the above-mentioned controls.	• Levels 4 and 5 of student data (See Use Guidelines for Student Data) • Grievances/disciplinary action records • Research, proposals, research plans and results to International Traffic in Arms Regulations/Export Administration Regulation (ITAR/EAR)
Confidential	This type includes data elements usually not disclosed to the public but are less sensitive than highly confidential data. If a legally required and applicable Colorado Open Records Act (CORA) request is submitted, these records may be released. Requirements when accessing, handling or storing: • Only share with the people who are authorized to use it for a legitimate business purpose. This includes verbal and written information.	• Faculty and staff personnel records, benefits, salaries, performance evaluations and employment applications • University insurance records • Donor contact data and non-public gift amounts • Fundraising data • Non-public policies • Internal memos and emails, and non-public reports

	• Ensure networks or systems used to handle or store the data have appropriate firewalls, monitoring, logging, patching, anti-malware, and related security controls. • Use university provided computers when accessing or processing data. If this is not possible and you must use a personal computer, use a remote desktop to connect to your university-provided computer.	• Purchase requisitions, cash records, budgetary plans • Non-public contacts • University and employee ID numbers • Levels 2 and 3 of student data (See Use Guidelines for Student Data) • Research proposals • Research plans and results • Internal/unpublished business documents
Public	This type includes any data on university websites to which the data trustee allows access without authentication and data made freely available through university print material.	• Directory data • Public policies • Published business documents •

<https://www.cu.edu/data-governance/resources-support/data-classification>

CU-SIS: data security levels

Types of Data Elements	Level 1 (Public)	Level 2 (Confidential)	Level 3 (Confidential)	Level 4 (Highly Confidential)	Level 5 (Highly Confidential)
Directory information	X				
All non-directory data not listed and work study information, gender identity, sex, pronouns, birth date, dorm, emergency Info, student ID, UUID, residency		X			
Military status, veteran's status, GPA, probation, suspension, COF, service indicators, address, phone number			X		
Disability, race, ethnicity, citizenship, legal presence, visas, religion				X	

SSN, NID, financial aid (except work study), loan and bank account numbers, health information, sexual orientation

<https://www.cu.edu/data-governance/resources-support/data-classification/student-data-use-guidelines>