A STUDENT PRIVACY PRIMER FOR
FACULTY, TEACHING ASSISTANTS, AND READERS

Student privacy at UC Davis is governed by federal and state laws (most notably the Family Educational Rights and Privacy Act of 1974, or, FERPA), institutional, and UC policy. As a general rule, presume that all student information is confidential, and do not disclose confidential student information without a student's signed written consent except to campus officials who have a *legitimate educational interest* in the information. Student privacy is the responsibility of every campus official who accesses, views, and uses confidential student data. Additional student privacy training is available at the UC Learning Center (http://lms.ucdavis.edu, search for "FERPA"); official student privacy policy may be found in the UC Davis PPM, Section 320-21.

Disclosures. While some information is considered public (i.e., disclosable by default – such as student name and phone number), students may designate that some or all of their student record be kept confidential. Disclosing student information counter to a confidentiality designation can have serious legal ramifications, and may even jeopardize the safety of the student. As such, it is a good idea to refer requests for student information to the Office of the University Registrar (studentprivacy@ucdavis.edu) or the Office of Campus Counsel (publicrecords@ucdavis.edu). If you receive a subpoena for student information, contact Campus Counsel right away.

Who has a legitimate education interest? A campus official has a legitimate educational interest in information only if the information is relevant and necessary for them to fulfill their role in the student's education. Faculty members are not entitled to access all information about their students; only that to which they have a legitimate educational interest.

Parents. Parents of university students do not have any special rights under FERPA and should not be given access to confidential student records without the student's written consent. Some campus systems, such as MyBill, allow students to grant their parents limited access to parts of their record, but such permission does not extend beyond these systems.

Student Right to Access and Review. Students have the right to access and review their own student records. Unless a record is specifically exempted by FERPA, such as employment or health records unrelated to student status, any document that refers to a student – even obliquely, such as by their initials or student ID number – is generally considered to be part of the student's record and subject to review by the student. An exception to this is a document that is kept in the sole possession of the person who created it (although it may still be subpoenaed).

DO NOT post graded, identifiable student work in the hallway or in an unmonitored area for students to pick up.

Posting of Grades or Other Student Work. Class rosters containing student photographs, student ID numbers, or other personally identifiable student information should not be posted publically. This includes student ID numbers, names, Social Security Numbers (never use the SSN for anything!), or other linkable identifiers. An alternative is to use an identifier that is only known to the instructor and the student, such as a unique exam number or class ID.

Privacy in the Classroom. Student disclosure restrictions do not apply to certain class-related disclosures. Students cannot refuse to identify themselves in class, nor can they prohibit disclosure of their identity in class or as part of a class roster or email list. Students cannot be anonymous in class, whether in-person, online, or in other forms of instruction. Students must disclose their name, student ID, and email address to their instructor or TA.

Websites and Cloud-based Services. Placing any confidential student information on a website or cloud-based service not under contract with the University may raise student privacy concerns. The use of these sites should not be required in class, and students concerned about their privacy should be allowed to provide their information to the instructor in a secure manner. Avoid requiring students to post identifiable work where it would be publicly available or available to other students in the class, unless this availability is part of the instructional pedagogy.

Re-disclosures. Do not re-disclose confidential student information to any other parties. If somebody else needs the information they should request it themselves from the originator of the data. If you are the originator of such information and are disclosing it to somebody, you should include a notice to this effect (a sample notice is available from the Office of the University Registrar).

Letters of Recommendation. When writing a letter of recommendation, limit the information disclosed in the letter to your own personal observations; do not include information from the student record, such as grades, without the student's written consent.

Disruptive Students and Emergencies. You may share information about distressed or disruptive students with University officials who have a legitimate educational interest in the information (for instance, Student Judicial Affairs or CAPS). In addition, in the event of a health or safety emergency, you can share information with other people, within and outside the University, to protect the health or safety of the student or others. Such disclosures should be noted on the affected student's record.

If you find a breach of student privacy has occurred or you have questions or concerns regarding student privacy, please contact the Office of the University Registrar at studentprivacy@ucdavis.edu.