CAL POLY

Human Resource Information System

ACCESS AND COMPLIANCE FORM - FACULTY

FACULTY EMPLOYEE:

I certify that I have received training on the appended state and federal laws and University policies that govern access to and use of information contained in employee, applicant, and student records, including data that is accessible through the PeopleSoft Human Resource System.

I understand that I am being granted access to this information and data based on my agreement to comply with the following terms and conditions:

- I will comply with the state and federal laws and University policies that govern access to and use of information contained in employee, applicant, and student records, including data that is accessible through the Human Resource Information System. While a current summary is attached, state and federal laws may be revised that may necessitate additional training and requirements.
- My right to access information and/or data is strictly limited to the specific information and data that is relevant and necessary for me to perform my job-related duties.
- I will maintain the privacy and confidentiality of the information and data that I obtain, including its storage and disposal.
- Before sharing information or data with others, electronically or otherwise, I will make reasonable efforts to ensure that the recipient is authorized to receive that information or data. I will sign off the Human Resource Information System prior to leaving the terminal/PC.
- I will keep my password(s) to myself, and will not disclose them to others unless my immediate supervisor authorizes such disclosure in writing.

I understand that if I intentionally misuse personal information or data that I obtain through my employment, I will be subject to disciplinary action up to and including termination.

I certify that I have read this Access and Compliance Form, I understand it, and I agree to comply with its terms and conditions.

_____	_____	_____
Name (please print)	Signature	Date

CAL POLY

Information Use and Confidentiality – A Compendium for Faculty

The University and its officials have a responsibility to protect confidential information about students and employees. Faculty, who have access to legally protected information about students, share in this responsibility. This outline will list and briefly describe the laws and policies established to define protected information and suggest some practices for faculty to carry out their responsibilities in this area. The discussion of laws and policies in this outline is by no means complete, but is intended as a summary of provisions useful to faculty at Cal Poly.. It is based upon the best understanding of the laws and policies by University staff; the laws and policies supersede any incorrect information in this outline.

The collective bargaining agreement between the California Faculty Association (CFA) and the CSU requires faculty unit employees to sign the "Human Resources Information System Access and Compliance Form -Faculty " dealing with confidentiality of campus records.

Why is this important?

Releasing protected information can result in embarrassment, identity theft, and potentially legal liability for faculty and the University. Faculty and staff who violate the laws, regulations, or policies concerning the privacy of information are subject to sanctions or to disciplinary action, up to and including termination.

Minimum standards of security, ethics, conduct, and protocol include:

- Respect for the privacy of other users
- Users shall not seek information on, obtain copies of, or modify files, data, or passwords of other users unless explicitly authorized to do so.
- Respect for copyright and license agreements
- Respect for the integrity of computing systems
- Users shall not develop programs that harass other users or infiltrate or damage other computers or systems.

What laws and policies cover this subject?

The list below is not exhaustive, but addresses the laws and policies most critical to faculty:

- State Information Practices Act of 1977
- Title 5, California Code of Regulations
- Cal Poly Confidentiality-Security Policy
- California Penal Code Section 502
- CSU Information Security Policy
- Cal Poly Information Technology Responsible Use Policy
- State Administrative Manual
- Family Educational Rights and Privacy Act (FERPA)
- "The Identity Theft and Assumption Deterrence Act of 1998" (18 U.S.C. 1028) makes identity theft a federal crime.
- "Wayne Shredding Bill" (State Civil Code 1798.80-82) –requires that sensitive information be unreadable before disposing of either electronic or paper documents.

98.29

- California Code 1798.29 requires notification for breach of security of personal information

Information Practices Act Overview

Each Campus and the Chancellor's Office have the legal responsibility to administer and comply with provisions of the State Information Practices Act of 1977. The law imposes specific requirements on state agencies relating to the collection, use, maintenance, and dissemination of information relating to individuals.

- *Careless, accidental, or intentional disclosure of information to unauthorized persons may result in disciplinary action against the responsible individual and civil action against CSU.*
- ***§1798.1*** *– "The Legislature declares that the right to privacy is a personal and* fundamental right protected by Section 1 of Article I of the California Constitution and by the United States Constitution….the maintenance and dissemination of personal information (must) be subject to strict limits."
- "Personal Information" is information that identifies or describes an individual, including name, social security number, physical description, home address and telephone number, education, financial matters, medical or employment history, and statements made by or attributed to the individual.
- §1798.20. Rules of conduct shall be established for people involved in the design, development, operation, disclosure, or maintenance of records containing personal information. People involved in the design, development, operation, disclosure, and maintenance of records containing personal information shall be instructed about the rules of conduct governing these activities, as well as the remedies and penalties for non-compliance.
- Except as authorized by statute, no agency (or individual associated with the agency) may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains.

INFORMATION PRACTICES ACT OF 1977

The Information Practices Act, Section 1798 of the California Civil Code, places specific requirements on state agencies in relation to the collection, use, maintenance and dissemination of information relating to individuals. Careless, accidental or intentional disclosure of information to unauthorized persons can have far-reaching effects, which may result in disciplinary action against those involved in unauthorized disclosure (Section 1798.55) and civil action against the CSU with a right to be awarded reasonable attorney's fees, if successful. For reference, the following ***summary of relevant provisions*** is provided:

Article 1: General Provisions and Legislative Findings

§1798.1 The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. The Legislature further makes the following findings:

a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.
b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.
c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.

Article 2: Definitions

§1798.3. As used in this chapter:

a) The term "personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual…
c) The term "disclose" means to disclose, release, transfer, disseminate, or otherwise communicate all or any part of any record orally, in writing, or by electronic or any other means to any person or entity.

Article 5: Agency Requirements

§1798.20. Each agency shall establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing personal information and instruct each such person with respect to such rules and the requirements of this chapter, including any other rules and procedures adopted pursuant to this chapter and the remedies and penalties for noncompliance.

§1798.21. Each agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of this chapter, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury.

Article 6: Conditions Of Disclosure
§1798.24. No agency may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains... [Exceptions to this rule are listed in the statute.]

Article 10: Penalties
§1798.55. ***The intentional violation of any provision of this chapter or any rules or regulations adopted thereunder, by an officer or employee of any agency shall constitute a cause for discipline, including termination of employment***. (Emphasis added.)

§1798.56. Any person who willfully requests or obtains any record containing personal information from an agency under false pretenses shall be guilty of a misdemeanor and fined not more that five thousand dollars ($5,000), or imprisoned not more than one year, or both.

Title 5, California Code of Regulations Overview

- *Personal Information should not be collected unless the need for it has been clearly established in advance.*
- *Personal information should be appropriate and relevant to the purpose for which it has been collected.*
- *Personal Information should not be transferred outside CSU unless such transfer is compatible with the disclosed purpose for which it was collected.*
- Personal Information should be used as a basis for a decision only when it is accurate and relevant.
- Precautions should be taken to prevent the unauthorized access to or use of personal information retained by CSU.

TITLE 5, CALIFORNIA CODE OF REGULATIONS

Sections 42396 through 42396.5 of Title 5 of the California Code of Regulations address privacy and the principles of personal information management applicable to the California State University. Title 5 can be found on the Web at: http://ccr.oal.ca.gov/. For reference, the following summary is provided:

§42396.2 Principles of Personal Information Management. The following principles of personal information management shall be implemented within The California State University:

(a) There should be no personal information system the existence of which is secret.
(b) Personal information should not be collected unless the need for it has been clearly established in advance.
(c) Personal information should be appropriate and relevant to the purpose for which it has been collected.
(d) Personal information should not be transferred outside The California State University unless the transfer is compatible with the disclosed purpose for which it was collected. (Emphasis added.)
(e) Personal information should be used as a basis for a decision only when it is accurate and relevant.
(f) There should be procedures established by which a person may learn what personal information about him or her has been retained by The California State University and where lawful, have those records disclosed to him or her, pursuant to the provisions of this Article.

(g) There should be established within The California State University procedures by which a person may request in writing addition to or deletion of personal information about himself or herself which does not meet the principles in this section. Such requests should be honored within a reasonable length of time or the person should be permitted to file a concise statement of dispute regarding the personal information which shall become a permanent part of the record, or, the disputed personal information should be destroyed.

(h) Precautions should be taken to prevent the unauthorized access to or use of personal information retained by The California State University. These principles shall be construed and implemented so as to be consistent with all federal and state laws otherwise regulating or allowing for the use of personal information, including but not limited to Education Code Section 89546 relating to employee records. (Emphasis added.)

CSU Information Security Policy Overview

- It is the policy of the CSU that all campuses and the Office of the Chancellor comply with applicable State and Federal laws regarding data security and privacy.
- The unauthorized modification, deletion, or disclosure of information included in CSU data files and data bases violates privacy rights and possibly constitutes criminal acts and is expressly forbidden. This applies to all students, faculty, and staff with access to this data.
- This policy applies to all CSU data systems and equipment containing private, confidential, or mission critical data.
- Each CSU campus must develop and maintain a written set of security policies and procedures that implement information security, confidentiality practices, and end user responsibilities.
- The policies and procedures of each CSU campus must provide for:
  --Use of resources for authorized, sanctioned, and approved activities only and sanctions for policy violations.
  --Individual unique user ID/passwords.
  --Access privileges controlled on a need to know basis.
- Password security requirements.
  --Appropriate protections for remote-access systems and applications.
  --Granting, reviewing, and removing access, as necessary and appropriate.

Cal Poly Confidentiality Security Policy

Access to computers and data is a privilege extended at the discretion of Cal Poly and the University retains the right and authority to revoke or restrict such privileges at any time. I agree to adhere to the established policy related to all Cal Poly data, screen security and confidentiality. I understand my professional responsibility includes trust and agree to perform my job in conformance with the security procedures of the University as stated below:

1. University computers will be used for authorized purposes only. All data processed is considered sensitive and/or confidential. This data is governed by federal, state and university policies. Access to data is based on the "need to know" philosophy that is directly related to my assigned duties at the University.
2. I understand that I am responsible for the security of whatever data I retrieve. I will provide all necessary safeguards to all sensitive and/or confidential information including reproduction, destruction or modification of data.
3. I have read the campus policies with regard to the summary of the Privacy Rights of Students in Education Records, California Penal Code Section 502, and the Information Practices Act of 1977 (appended) and will abide by those regulations.
4. I understand that I am to restrict my retrieval and other computing activities only to data I have been specifically permitted to access as related to my assigned duties and using only functions and utilities which I have been authorized and trained to use.
5. I understand that my account and password are issued for my exclusive use only and I am responsible for the security thereof. An assigned password shall not be shared with, or delegated to others. I understand that I am also responsible for any student assistant, temporary help and/or production accounts issued in my name.
6. I understand that if I move to another department on campus, I will retain the same account number and password, although my security access may change.
7. I understand that if my relationship with the University is terminated for any reason, I will no longer have access to University equipment and data.

Failure to abide by this agreement may result in my access and/or account being restricted**,** denied or discontinued. I further understand that illegal access of data may be a violation of the California Penal Code 502 and/or the Information Practices Act of 1977 and therefore punishable up to and including dismissal from position, fine and/or imprisonment.

CALIFORNIA PENAL CODE SECTION 502

Computer crimes: Status as felonies: (b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense. (c) Any person who maliciously accesses, alters, deletes, damages or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense. (d) Any person who violates the provisions of subdivision (b) or (c) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment."

State Administrative Manual

§4841.6 RESPONSIBILITY OF CUSTODIANS OF INFORMATION

The responsibilities of a custodian of an automated file or database consist of:

- Complying with applicable law and administrative policy;
- Complying with any additional security policies and procedures established by the owner of the automated information and the agency Information Security Officer;
- Advising the owner of the information and the agency Information Security Officer of vulnerabilities that may present a threat to the information and of specific means of protecting that information; and
- Notifying the owner of the information and the agency Information Security Officer of any actual or attempted violations of security policies, practices and procedures.

§4841.7 RESPONSIBILITY OF USERS OF INFORMATION

The responsibilities of a user of information consist of:

- Using state information assets only for state purposes;
- Complying with applicable laws and administrative policies (including copyright and license requirements), as well as any additional security policies and procedures established by the owner of the information and the agency Information Security Officer; and
- Notifying the owner of the information and the agency Information Security Officer of any actual or attempted violations of security policies, practices and procedures.

Family Educational Rights and Privacy Act (FERPA)

The law defines several types of information:

- "Directory information" is public unless student has requested that it not be disclosed.
- "Education records" may be disclosed only to certain individuals and agencies without the student's permission.
- "Sole possession" notes are made by one person as an individual observation or recollection, are kept in the possession of the maker, and are shared with no one but a temporary substitute. Instructional and supervisory notes are an excellent example of sole possession notes.

Directory information is defined by the university within the law's limits. Typical information includes (the following is NOT comprehensive):

Name
Class level (freshman, graduate student)
Degree type and date
Dates of attendance
Honors
E-mail address

Directory information may NOT include:

Social Security Number or student identification number
Race or gender
Grades or GPA
Country of citizenship
Religion

Admissions and Records keeps records of student requests for non-disclosure, and faculty have no easy way to know whether a request not to disclose directory information has been made.

Education records are those records directly related to a student and maintained by the university or by a party acting for it. Education records are NOT sole possession records, law enforcement unit records, employment records, medical records, or post-attendance records.

Some suggestions for faculty practices under FERPA

Posting or release of grades

- Posting of grades, such as on an office door, whether with directory information (name) or education record identifiers (Social Security Number or student identification number) where they can be seen by those other than the student or a school official with a legitimate educational interest violates FERPA. Some solutions: (a) agreeing upon code numbers or words known only to the individual student and the faculty member, (b) mailing grades in a sealed envelope, or (c) informing students of the day that you will be entering grades into PeopleSoft and reminding them that they can retrieve their own grade information over the Internet.
- When returning tests or papers in class, take common sense precautions to ensure privacy of the grade information.
- Do not leave final papers or exams in a box outside your office door. This not only shares grade information inappropriately, it also opens up the possibility that "A" papers may be stolen and plagiarized by other students. Ask students who want their final papers or exams back to give you a pre-addressed, stamped envelope, or offer to return them during office hours the following semester.
- When disposing of papers or exams that students do not wish returned, it's best to shred them.

Class directories

- It is common to circulate class directories listing student names and contact information (e.g., e-mail address). Requiring such information to be shared with the class may create conflicts with a student's request to withhold directory information.
- If you use such directories, state clearly that, if students have any concerns, they may discuss them with you after class. Consider encouraging the student to use a yahoo or hotmail account for the class or other techniques that will permit the student to maintain privacy of this information.

(more on next page)

Students of federally funded universities have the right to inspect, review, and seek correction of their education records. Students reviewing their records do not have access to parts of records containing information about other students.

Except as provided in the law, education records may not be released without the student's explicit, written permission. Student permission to release education records generally applies to the specific recipient, purpose, and release period. Most of the exceptions in the law allowing release of records without student permission apply to common actions of administrative offices (Admissions and Records, Financial Aid, etc.) only.

School officials may obtain education record information, provided that they have a legitimate educational interest. Faculty are school officials. Note that both tests are important:

Status as a school official, and
Legitimate educational interest in the specific record.

Employment Contracts Overview

- FERPA treats student employment (student assistants, work study trainees, Graduate Assistants, Teaching Associates) as education record information that may not be released without student permission, except to agencies as provided in the law.
- Under the Information Practices Act, employment contracts of all other State employees are public record.
- An individual's name, pay title, time base, dates of employment, and gross pay rate are public record and must be released to any member of the public.
- Other employment-related information such as net pay or performance information is private and may be released only with written permission from the individual or as provided in law.

Suggestions, continued

Letters of Recommendation

- Letters of recommendation are a part of the student's education record. The student must grant permission for the release of the information from the education record. The letter will be available to the student unless s/he has waived the right of access, in writing.
- The written request for a letter of recommendation should contain:
  - The person/agency to whom the information is to be released.
  - The purpose of the letter of recommendation.
- Whether or not the student is waiving his/her right to review a copy of the letter.
- SIS+ carries a student's request to disclose/not disclose "directory information"

Meetings with students

- Faculty commonly meet with students in their offices with the door open. During such meetings, incautious conversation about the student's education record, or showing the record in a way that is visible to others, can constitute a prohibited release of the student's education record.
- Consider the arrangement of the office, the placement of chairs in the hall for students waiting to meet, and other techniques for preserving the student's right to privacy.

Protecting the privacy of your grade book and notes

- Generally, your grade book and notes about students are "sole possession" records. Sharing these notes with another person or placing them where they can be viewed by others makes them "education records" and available to the student.
- If you need to discuss student problems with others (e.g., department chair or student discipline staff), do not share your notes directly; rather, summarize the problem.