HUMBOLDT STATE UNIVERSITY

Information Use and Confidentiality – An outline for use by faculty

March 9, 2005

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 (adapted from a version developed by Sonoma State University and used with its permission) lists, and briefly describes, the laws and policies established to define protected information and suggest some practices for faculty to use in carrying 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 Humboldt State University. 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.

Why is this important?

Releasing protected information can result in embarrassment, identity theft, and potentially legal liability for faculty and the University.

On March 27, 2003, Chancellor Charles Reed issued a memorandum that:

- Expresses concern over the privacy of confidential student and employee data.
- Requires the certification and approval of persons requiring access.
- Requires the signing of a Confidential Information System Access Agreement.
- Requires periodic audits.
- Announces that PeopleSoft and CSU will be identifying and implementing solutions.

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.

What laws and policies cover this subject?

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

- "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.
- Family Educational Rights and Privacy Act (FERPA)
- State Information Practices Act of 1977
- Title 5, California Code of Regulations
- CSU Information Security Policy
- CENIC/DCP Acceptable Use Policy
- State Administrative Manual

Family Educational Rights and Privacy Act (FERPA)

The law defines several types of information:

- "Directory information" is public unless the 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.

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) sending grades via email. Note that final grades do not need to be distributed because they are available to the student via the Web.
- 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 is 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)

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.

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:

(1) Status as a school official, and
(2) Legitimate educational interest in the specific record.

Policy for compliance with FERPA at Humboldt State University is given in University Management Letter 03-03, Student Records Access Policy, dated September 2003. You can read this policy online at:

http://www.humboldt.edu/~hsupres/uml/uml03-03.html

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.

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 use student graders, have them give you the grading results so that you can enter the information.
- 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.

Information Practices Act

All campuses and the Office of the Chancellor 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 the 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.

Employment Contracts

- 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.

Title 5, California Code of Regulations

- 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 the 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 the CSU.

CSU Information Security Policy

- 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.

CENIC/DCP Acceptable Use Policy

- The Corporation for Education Network Initatives in California (CENIC) administers the Internet service used by the University. Any computer traffic that comes into or leaves the campus – web traffic, e-mail, or other – travels on CENIC's systems.
- The goal of the CENIC/DCP Acceptable Use Policy is to ensure that all uses are consistent with the stated purpose, mission, and goals.
- Member institutions are expected to honor the rights of other users, respect the integrity of the systems and related physical resources, and observe relevant laws, regulations, and contractual obligations.
- Information resources accessed or delivered through CENIC will be used by members of its community with respect for the public trust and academic freedom, and in accordance with policy and regulations established by the CSU, the State of California, and Humboldt State University.
- Member institutions and their users follow normal standards of security, ethics, conduct, and protocol when using CENIC.
- 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.

Information on general acceptable uses and unacceptable uses of CENIC can be found on pages 11 and 12 of this material.

State Administrative Manual

The State Administrative Manual, in Sections 4841.6 and 4841.7, outlines responsibilities for the custodians and users of information. These include:

- using information assets only for state purposes;
- complying with applicable law and administrative policy as well as 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 ISO of vulnerabilities that may present a threat to the information, as well as means to thwart that threat; and
- notifying the owner of the information and the ISO of any actual or attempted violations of security policies, practices, or procedures.

Excerpts of Laws and Regulations Concerning Privacy of Data

Family Educational Rights and Privacy Act

20 USC S. 1232g

§1232g. Family educational and privacy rights
(a) Conditions for availability of funds to educational agencies or institutions; inspection and review of education records; specific information to be made available; procedure for access to education records; reasonableness of time for such access; hearings; written explanations by parents; definitions.

(1) (A) No funds shall be made available under any applicable program to any educational agency or institution which has a policy of denying, or which effectively prevents, the parents of students who are or have been in attendance at a school of such agency or at such institution, as the case may be, the right to inspect and review the education records of their children. If any material or document in the education record of a student includes information on more than one student, the parents of one of such students shall have the right to inspect and review only such part of such material or document as relates to such student or to be informed of the specific information contained in such part of such material. Each educational agency or institution shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children within a reasonable period of time, but in no case more than forty-five days after the request has been made.

(B) The first sentence of subparagraph (A) shall not operate to make available to students in institutions of postsecondary education the following materials:

(i) financial records of the parents of the student or any information contained therein;

(ii) confidential letters and statements of recommendation, which were placed in the education records prior to January 1, 1975, if such letters or statements are not used for purposes other than those for which they were specifically intended;

(iii) if the student has signed a waiver of the student's right of access under this subsection in accordance with subparagraph (C), confidential recommendations--

(I) respecting admission to any educational agency or institution,

(II) respecting an application for employment, and

(III) respecting the receipt of an honor or honorary recognition.

(C) A student or a person applying for admission may waive his right of access to confidential statements described in clause (iii) of subparagraph (B), except that such waiver shall apply to recommendations only if (i) the student is, upon request, notified of the names of all persons making confidential recommendations and (ii) such recommendations are used solely for the purpose for which they were specifically intended. Such waivers may not be required as a condition for admission to, receipt of financial aid from, or receipt of any other services or benefits from such agency or institution.

(2) No funds shall be made available under any applicable program to any educational agency or institution unless the parents of students who are or have been in attendance at a school of such agency or at such institution are provided an opportunity for a hearing by such agency or institution, in accordance with regulations of the Secretary, to challenge the content of such student's education records, in order to insure that the records are not inaccurate, misleading, or otherwise in violation of the privacy or other rights of students, and to provide an opportunity for the correction or deletion of any such inaccurate, misleading, or otherwise inappropriate data contained therein and to insert into such records a written explanation of the parents respecting the content of such records.

(3) For the purposes of this section the term "educational agency or institution" means any public or private agency or institution which is the recipient of funds under any applicable program.

(4) (A) For the purposes of this section, the term "education records" means, except as may be provided otherwise in subparagraph (B), those records, files, documents, and other materials which--

(i) contain information directly related to a student; and

(ii) are maintained by an educational agency or institution or by a person acting for such agency or institution.

(B) The term "education records" does not include--

(i) records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute;

(ii) records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement.

(iii) in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or

(iv) records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.

(5) (A) For the purposes of this section the term "directory information" relating to a student includes the following: the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student.

(B) Any educational agency or institution making public directory information shall give public notice of the categories of information which it has designated as such information with respect to each student attending the institution or agency and shall allow a reasonable period of time after such notice has been given for a parent to inform the institution or agency that any or all of the information designated should not be released without the parent's prior consent.

(6) For the purposes of this section, the term "student" includes any person with respect to whom an educational agency or institution maintains education records or personally identifiable information, but does not include a person who has not been in attendance at such agency or institution.

(b) Release of education records; parental consent requirement; exceptions; compliance with judicial orders and subpoenas; audit and evaluation of Federally-supported education programs; recordkeeping.

(1) No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of educational records (or personally identifiable information contained therein other than directory information, as defined in paragraph (5) of subsection (a)) of students without the written consent of their parents to any individual, agency, or organization, other than to the following--

(A) other school officials, including teachers within the educational institution or local educational agency, who have been determined by such agency or institution to have legitimate educational interests;

(B) officials of other schools or school systems in which the student seeks or intends to enroll, upon condition that the student's parents be notified of the transfer, receive a copy of the record if desired, and have an opportunity for a hearing to challenge the content of the record;

(C) authorized representatives of (i) the Comptroller General of the United States, (ii) the Secretary, (iii) an administrative head of an educational agency (as defined in section 408(c) , or (iv) State educational authorities, under the conditions set forth in paragraph (3) of this subsection;

(D) in connection with a student's application for, or receipt of, financial aid;

(E) State and local officials or authorities to whom such information is specifically required to be reported or disclosed pursuant to State statute adopted prior to November 19, 1974;

(F) organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction, if such studies are conducted in such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations and such information will be destroyed when no longer needed for the purpose for which it is conducted;

(G) accrediting organizations in order to carry out their accrediting functions;

(H) parents of a dependent student of such parents, as defined in section 152 of the Internal Revenue Code of 1954; and

(I) subject to regulations of the Secretary, in connection with an emergency, appropriate persons if the knowledge

of such information is necessary to protect the health or safety of the student or other persons.

Nothing in clause (E) of this paragraph shall prevent a State from further limiting the number or type of State or local officials who will continue to have access thereunder.

(2) No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in education records other than directory information, or as is permitted under paragraph (1) of this subsection unless--

(A) there is written consent from the student's parents specifying records to be released, the reasons for such release, and to whom, and with a copy of the records to be released to the student's parents and the student if desired by the parents, or

(B) such information is furnished in compliance with judicial order, or pursuant to any lawfully issued subpoena, upon condition that parents and the students are notified of all such orders or subpoenas in advance of the compliance therewith by the educational institution or agency.

(3) Nothing contained in this section shall preclude authorized representatives of (A) the Comptroller General of the United States, (B) the Secretary, (C) an administrative head of an education agency or (D) State educational authorities from having access to student or other records which may be necessary in connection with the audit and evaluation of Federally-supported education program, or in connection with the enforcement of the Federal legal requirements which relate to such programs: Provided, That except when collection of personally identifiable information is specifically authorized by Federal law, any data collected by such officials shall be protected in a manner which will not permit the personal identification of students and their parents by other than those officials, and such personally identifiable data shall be destroyed when no longer needed for such audit, evaluation, and enforcement of Federal legal requirements.

(4) (A) Each educational agency or institution shall maintain a record, kept with the education records of each student, which will indicate all individuals (other than those specified in paragraph (1)(A) of this subsection), agencies, or organizations which have requested or obtained access to a student's education records maintained by such educational agency or institution, and which will indicate specifically the legitimate interest that each such person, agency, or organization has in obtaining this information. Such record of access shall be available only to parents, to the school official and his assistants who are responsible for the custody of such records, and to persons or organizations authorized in, and under the conditions of, clauses (A) and (C) of paragraph (1) as a means of auditing the operation of the system.

(B) With respect to this subsection, personal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student.

(5) Nothing in this section shall be construed to prohibit State and local educational officials from having access to student or other records which may be necessary in connection with the audit and evaluation of any federally or State supported education program or in connection with the enforcement of the Federal legal requirements which relate to any such program, subject to the conditions specified in the proviso in paragraph (3).

(6) Nothing in this section shall be construed to prohibit an institution of postsecondary education from disclosing, to an alleged victim of any crime of violence (as that term is defined in section 16 of title 18, United States Code), the results of any disciplinary proceeding conducted by such institution against the alleged perpetrator of such crime with respect to such crime.

(c) Surveys or data-gathering activities; regulations. The Secretary shall adopt appropriate regulations to protect the rights of privacy of students and their families in connection with any surveys or data-gathering activities conducted, assisted, or authorized by the Secretary or an administrative head of an education agency. Regulations established under this subsection shall include provisions controlling the use, dissemination, and protection of such data. No survey or data-gathering activities shall be conducted by the Secretary, or an administrative head of an education agency under an applicable program, unless such activities are authorized by law.

(d) Students' rather than parents' permission or consent. For the purposes of this section, whenever a student has attained eighteen years of age, or is attending an institution of postsecondary education the permission or consent required of and the rights accorded to the parents of the student shall thereafter only be required of and accorded to the student.

(e) Informing parents or students of rights under this section. No funds shall be made available under any applicable program to any educational agency or institution unless such agency or institution informs the parents of students, or the students, if they are eighteen years of age or older, or are attending an institution of

postsecondary education, of the rights accorded them by this section.

(f) Enforcement; termination of assistance. The Secretary, or an administrative head of an education agency, shall take appropriate actions to enforce provisions of this section and to deal with violations of this section, according to the provisions of this Act, except that action to terminate assistance may be taken only if the Secretary finds there has been a failure to comply with the provisions of this section, and he has determined that compliance cannot be secured by voluntary means.

(g) Office and review board; creation; functions. The Secretary shall establish or designate an office and review board within the Department of Health, Education, and Welfare for the purpose of investigating, processing, reviewing, and adjudicating violations of the provisions of this section and complaints which may be filed concerning alleged violations of this section. Except for the conduct of hearings, none of the functions of the Secretary under this section shall be carried out in any of the regional offices of such Department.

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

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

The Board of Trustees (BOT) of the California State University (CSU) is responsible for protecting the confidentiality of information in the custody of the CSU; the security of the equipment where this information is processed and maintained; and, the related privacy rights of the CSU students, faculty and staff concerning this information. It is also the collective responsibility of the CSU, its executives and managers to insure:

- the integrity of the data;
- the maintenance and currency of the applications;
- the preservation of the information in case of natural or man-made disasters; and,
- compliance with Federal and State regulations, including intellectual property and copyright.

This policy applies to all students, faculty and staff, consultants employed by the CSU or any other person having access to CSU information technology resources. The unauthorized modification, deletion, or disclosure of information included in CSU data files and data bases can compromise the integrity of CSU programs, violate individual privacy rights and possibly constitute a criminal act, and is expressly forbidden.

This responsibility is delegated to the campus Presidents in accordance with CSU policies. It is anticipated that the President will assign most or all of the responsibility for policy enforcement to the CIO/ITAC Designee. Therefore, the ITAC designee should keep the President informed of any changes of security and confidentiality procedures affecting the campus information technology environment. However, this policy is not limited to those systems and equipment operated and maintained by the central Information Technology organization. It applies to all data systems and equipment on campus that contain data deemed private or confidential and/or which contain mission critical data, including departmental, divisional and other ancillary systems and equipment.

SECURITY PROCEDURES

Each campus and the Chancellor's Office must develop and maintain a written set of security policies and procedures that at a minimum implement information security, confidentiality practices consistent with these policies, and end-user responsibilities for the physical security of the equipment and the appropriate use of hardware, software and network facilities.

SECURITY POLICIES

1) It is the policy of the CSU that all computer equipment, hardware and software be physically secure. Campuses must have plans and procedures for data centers and shared computing environment that insure, where appropriate:

   a) Protection against natural/accidental disasters.
   b) Protection against intentional disasters.

2) It is the policy of the CSU that Data (Information) be secure. Campus plans must include, where appropriate:

   a) Definitions and Descriptions of:
      i) Critical applications (as defined in the State Administrative Manual).
      ii) Critical information.
      iii) Other critical resources.
   b) Procedures for:
      i) The implementation of cost/effective data security systems (RACF, firewalls, routers, etc.).
      ii) Insuring the confidentiality and security of all information deemed confidential and private
      iii) Backup and off-site storage of mission critical data
   c) Required Security Measures which include
      i) Protection against known vulnerabilities.
      ii) Testing of security procedures in data centers and shared computing environments.
      iii) Organization and administration.
      iv) Control of operating system software.
      v) Control of application software and data.
      vi) Control of Transaction systems.
      vii) Control of Database systems.
      viii) Control of magnetic media storage in data centers and shared computing environments
   d) Guidelines for System Design:
      i) Completeness of data.
      ii) Integrity of data.
      iii) Accuracy of data.
      iv) Audit trails of critical data changes (grade changes, residency determination, etc.).

3) It is the policy of the CSU that all campuses have appropriate personnel policies and procedures relative to employees who have physical or virtual access to information technology equipment or the data residing therein. These policies and procedures should provide for:
   i) Use of resources for authorized, sanctioned and approved activities only and sanctions for policy violations.
   ii) Individual unique user ID/passwords (no shared IDs).
   iii) Access privileges controlled on a need to know basis (files, records, data elements, data bases, applications, screens, terminals, etc.).
   iv) Password Security Requirements
   v) Appropriate protections for systems and applications accessible by remote access and/or dial –up modem.
   vi) Assignment of responsibilities (access privileges granted)
   vii) Reassignment of responsibilities (access privileges reviewed).
   viii) Termination of employment (access privileges removed).

4) 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 Corporation for Education Network Initiatives in California (CENIC) *and* Digital California Project (DCP) Acceptable Use Policy

The full Acceptable Use Policy is available at http://www.cenic.org/downloads/pmo/AUP1.pdf.

Introduction:

One of the goals of CENIC, through the DCP, is to provide K-12 schools, school districts and county offices of education and other institutions…with access to a high-speed backbone network infrastructure that interconnects those sites with each other and to information and communication resources worldwide….The intent of the DCP Acceptable Use Policy (AUP) is to ensure that all uses are consistent with DCP's status purpose, mission, and goals. The AUP does not articulate all required or proscribed behavior by DCP participants, but it provides a framework of appropriate use within which users are required to honor the rights of other users, respect the integrity of the systems and related physical resources, and observe relevant laws, regulations, and contractual obligations….

Use of the DCP to access or deliver information resources will respect the principles of public trust and academic freedom, and will comply with policies and regulations established by CENIC and with local, state and federal laws.

General Acceptable Use:

Examples of acceptable use include, but are not limited to, the following:

- Activities that are part of the support infrastructure needed for instruction, scholarship and institutional management…
- Instructional applications engaged in by students, faculty and staff.
- Communication and exchange for professional development, to maintain currency, or to debate issues in a field or sub-field of knowledge.
- Subject matters/discipline associations, government-advisory, or standard activities related to the user's research, instructional and/or administrative activities.
- Applying for or administering grants or contracts…
- Announcements of new products or services used in instruction and institutional research.
- Access to information resources, computers, and people throughout the world.
- Interaction with students, faculty, and staff…
- Access to libraries, information resources, databases, and news…
- Importation of licensed software or other copyrighted materials for fair use or with permission.
- Administrative, academic, and research-related discussion groups.
- E-commerce activities in support of the administrative and academic programs of participant institutions.

Unacceptable Uses:

Examples of unacceptable uses include, but are not limited to, the following:

- Any illegal use of DCP, or use in support of illegal activities….Illegal use shall be defined as use that violates local, state and/or federal law….stalking others, transmitting or originating any unlawful, fraudulent or defamatory communications, transmitting copyrighted material beyond the scope of fair use without permission of the copyright owner, or any communications where the message or its transmission or distribution, would constitute or would encourage conduct that is a criminal offense.
- Activities that interfere with or disrupt network users, services, or equipment….distribution of unsolicited advertising or mass mailings; "spamming;" propagation of computer worms or viruses; and using DCP to make or attempt to make unauthorized entry to other computational, informational or communications devices or resources.
- Use in furtherance of profit-making activities (consulting for pay, sales or distribution of commercial products or services for profit, etc.) or use by for-profit companies, unless specifically authorized by the DCP Program Steering Committee and CENIC Board of Directors.
- Use in support of partisan political activities.
- Use for private or personal activities that exceed DCP related research, instruction, or administrative applications, or when there is personal monetary gain.

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.