Administrative Procedure

Number:	023
Effective:	6/17/85
Supercedes:	
Page:	1 of

Subject: INFORMATION PRACTICES

1.0. PURPOSE:

To establish the policy and procedure governing compliance of the campus with all relevant federal and state regulations for information practices.

2.0. ORGANIZATIONS AFFECTED:

2.1. All units of the University, except auxiliary organizations and Unit 3 (Faculty) employees.

2.2. Important: This procedure, or portions thereof, may be superseded by an agreement between The California State University and an exclusive employee representative.

When referring to this procedure as it relates to actions affecting represented employees, consult the appropriate Administrative Procedure which makes specific citation to applicable collective bargaining agreement sections.

3.0. REFERENCES:

3.1. State of California Civil Code, Title 1.8, Section 1798 of Part 4 of Division 3 (Information Practices Act).

3.2. 20 U.S.C. 12329 (Family Education Rights and Privacy Act of 1974).

3.3. California Education Code, Sections 24317.

3.4. Government Code, Sections 6250 et seq. (California Public Records Act.).

3.5. State Administrative Manual (SAM), Section 4843 (Information Security Officer.)

3.6. Office of the Chancellor Executive Order Number 382, Subject: Privacy and Personal Information Management--Student Records Administration.

Approved: **Date:**

3.7. Office of the Chancellor memoranda:

3.7.1. IS 81-25, Subject: Computer Security.

3.7.2. IS 78-20, Subject: Privacy and Personal Information Management--Automated Records.

3.7.3. BA 84-14, Subject: Public Safety Records Disposition--Authority for Public Safety Directors to Decide Retention/Destruction Periods.

3.7.4. BA 78-16, Subject: Privacy and Personal Information Management--Miscellaneous Records.

3.7.5. EVC 78-04, Subject: Information Practices.

3.7.6. FSA 78-68, Subject: Public Records Act--Personal Information.

3.7.7. FSA 78-38, Subject: Information Practices Act of 1977(SB 170 Roberti).

3.7.8. FSA 76-93 and Supplement 1, Subject: SB 1588 (Roberti), Employee Records.

3.7.9. PS 78-01, Subject: Law Enforcement Records Management-Privacy and Access.

3.8. Cal State L.A. Administrative Procedures:

3.8.1. Subject: Record Retention and Disposition

3.8.2. Subject: Destruction of Confidential Records

3.8.3. Subject: Personnel Files (In development)

3.8.4. Subject: Public Records (In development)

3.8.5. Subject: Student Records Administration

3.8.6. Subject: Vital Records Protection (In development)

3.9. Faculty Handbook. California State University, Los Angeles, Section: Personnel Files and Other Employment Records.

4.0. POLICY:

4.1. Information Practices Officer--The University will comply with the Information Practices Act of 1977. In order to ensure full implementation of the Act, the President will designate an Information Practices Officer to review all campus practices with regard to the collection, storage, use and transfer of records containing information about employees, students and visitors.

4.2. Access to Records--All individuals who are the subject of records maintained by this campus shall have the right to inquire and be notified as to whether or not a record pertaining to them is maintained. Whenever the campus is unable to access a record by reference to name only, or when access by name only would impose an unreasonable administrative burden, the requesting individual may be required to submit other identifying information necessary to facilitate access to the record.

4.2.1. Upon proper identification, any individual who requests access to a record pertaining to himself or herself will be granted access as quickly as is reasonably and practically possible, but in no event later than thirty (30) days of the request for active records or sixty (60) days for stored records. (See also Section 4.9., Public Records)

4.2.2. Individuals shall be allowed to review copies of the reports that are required to be filed with the Office of Information Practices relating to the type of records maintained by this campus.

4.2.3. Any notice to an individual which indicates that the campus maintains a record on that individual shall include the title and business address of the person directly responsible for the system of records of which the record is a part.

4.3. Photocopies of Records--If an individual wishes to have copies of records pertaining to himself or herself, such copies shall be made with a service charge of ten (10) cents per page. Copies of the requested records should be furnished to the subject individual within fifteen (15) days of the request.

Copies will be furnished directly to the individual, if practical, or to another person specifically authorized by the individual. Copies may be mailed to an address given by the requesting individual. In all cases, proper identification of the requestor is necessary to insure privacy.

When an individual is permitted to review or is given copies of information about himself or herself, any coincidental personal information relating to another individual shall be deleted or made unreadable.

4.4. Refusal of Access--If the campus refuses access to an individual based on the information being "confidential", the record custodian shall inform the individual of that fact. If the individual requests a review of a refusal of access, the Information Practices Officer shall make such review within thirty (30) days of such request and inform the individual in writing of its final decision.

4.5. Amendments to Records--Any request by an individual to amend or correct personal information in a record maintained by the University shall be answered within thirty (30) days from the date of the receipt of the request.

If the individual protests the University's refusal to make the requested changes to a record, the administrator or designee, shall review the refusal and make a final determination on the issue within thirty (30) days of the date of the request for review. For good cause the administrator may extend the review period by up to thirty (30) days.

If a final determination is made to sustain the refusal to make the requested changes, the University will permit the individual to file a statement of reasonable length setting forth the reasons for the individual's disagreement with the record. The statement shall become part of the individual's record and be disclosed with any authorized disclosures of such records. Should a dispute arise regarding the length of the statement, the Information Practices Officer will determine what is reasonable.

4.6. Disclosure--Records will be kept on all disclosures of personal and confidential records. The University is required to maintain a log of disclosures for three (3) years.

Section 1798.24 of the Information Practices Act outlines the circumstances under which personal or confidential information may be disclosed to persons other than the subject. It should be noted that certain employment information, such as name, salary range, etc., is public record information and not subject to the same protection as the personal or confidential categories.

4.7. Any off-campus contractor operating or maintaining campus records shall be bound by the same rules, regulations, and procedures pertaining to the security and confidentiality of records containing personal or confidential information as are employees of the University.

4.8. Mailing Lists--Individuals will be notified at the point of collection that the information they are providing may also be used for the purpose of generating mailing lists. The collection instrument will give the individual an option to have or not have name and address released. Upon the indication of exclusion, the individual's name and address shall be removed from a mailing list unless the name is used exclusively by the University to directly contact the individual.

4.9. Public Records--Public records are open to inspection at all times during University office hours and every citizen has a right to inspect any public record which does not come within an exempted category. An exact copy of the public record will be provided within ten (10) days unless impractical to do so following receipt of the request and payment of the service charge for copies. In unusual circumstances, this time limit may be extended up to ten working days as required for proper processing of the request.

The Administrative Procedure on Personnel Files lists those items considered to be public information that may be released to individuals requesting employment verification.

5.0. DEFINITIONS:

5.1. Access - As defined by the Information Practices Act, means a personal inspection and review of an individual's records, or a copy of an individual's records, or an oral or written description of the contents of an individual's records.

5.2. Automated - Records, files, and systems maintained through the use of a computer.

5.3. Confidential Information—As defined by the Information Practices Act, means information containing medical, psychiatric, or psychological material if the holder of the record determines that disclosure of the information would be medically or psychologically detrimental to the individual. Confidential information may be disclosed to a physician, psychiatrist, or other licensed medical or psychological personnel designated by the data subject if the campus has received written authorization signed by the individual.

5.4. Disclosure - As defined by the Information Practices Act, means permitting access, release, or transfer of personally identifiable information from an individual's records.

5.5. File - A collection of records.

5.6. Miscellaneous Records - Manually maintained or automated records containing personal or confidential information which are not addressed by the specific references noted above in Section 3.0. for student or personnel records. Examples are records for former students (alumni), the associated clinic, donors, friends of the library, and athletics.

5.7. File Owner - The office and/or manager who has responsibility for maintenance of the file and authority to permit others to have access to the file.

5.8. Personal Information - As defined by the Information Practices Act, means any information about an individual, but not limited to, the individual's education, employment history, financial transactions, medical or behavioral history that contains name, identification number, or other identifying particular.

5.9. Public Records - Any "writing" containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. "Writing" is further defined in the Public Records Act to include electronic media.

5.10. Record - Any grouping of information about an individual.

5.11. Record Custodian - Academic or administrative department head responsible for maintaining record systems. In instances where an individual in a department other than the department head is responsible for the day-to-day maintenance of a record system, the overall responsibility for the accuracy of the data will remain with the academic or administrative department head.

5.12. System - A collection of files.

6.0. RESPONSIBILITIES:

6.1. The President will designate a Dean or Senior Administrative level employee to serve as the Information Practices Officer.

6.2. The Information Practices/Security Officer will:

6.2.1. Coordinate the identification of campus forms and records which solicit personal or confidential information from individuals and maintain an index of such records.

6.2.2. Coordinate the development and implementation of appropriate personal information management policies, practices, and forms.

6.2.3. Assist in the resolution of questions regarding the legal authority for the collection, maintenance, and transfer of information.

6.2.4. Review the annual notice of record systems to the Office of Information Practices for completeness and appropriate responses.

6.2.5. Assist individuals in identifying and gaining access to records which may contain information about them.

6.2.6. Upon receiving a complaint, investigate whether any violation of procedures is involved, report the incident to the appropriate official, and recommend an appropriate resolution.

6.2.7. Investigate reported security or privacy violations which may involve personal or confidential records.

6.2.8. Serve as the primary liaison with the Information Practices Coordinator at the Chancellor's Office and State level.

6.2.9. Coordinate the removal of unnecessary and irrelevant personal and confidential information from departmental records.

6.3. Records Custodians and Owners of Automated Files (as defined in Sections 5.11) will:

6.3.1. As record systems are initiated or changed, notify the Information Practices Officer of changes required on the Personal / Confidential Records Report (Appendix 8.1) and determine who is responsible for approving and providing access.

6.3.2. Purge files of unnecessary or irrelevant information if directed to do so by the Information Practices Officer.

6.3.3. Inform departments administering any record system of the Rules of Conduct for University Employees found in Appendix 8.2.

6.3.4. Utilize the Privacy Notice when soliciting personal or confidential information from individuals. The information to be entered must be consistent with the data reported to the Information Practices Officer on the Personal / Confidential Records Report for that record.

6.3.5. Follow established procedures for access, review of access denials, and disclosures.

6.3.6. Maintain a log of access and movement/transfer of records.

6.3.7. Instruct the Computer Center regarding corrections and changes which should be made to permits for physical release of files and changes to access codes/label checks.

6.3.8. Delete names from mailing lists at data subject request.

6.4. Department Administrators will:

6.4.1. Route all new forms or revisions to existing forms which collect personal or confidential information to the Information Practices Officer for a review of the privacy notice.

6.4.2. Develop procedures for conducting periodic inventories of personal or confidential record systems.

6.4.3. Provide new employees with copies of procedures for managing personal or confidential information and obtain written acknowledgement that they have read and understood them. Periodic information practices refresher sessions should be held with current employees.

6.5. The Director of Data Processing and Network Operations will:

6.5.1. Identify the owner of each automated file containing personal or confidential information and develop procedures whereby access to the file must require appropriate recognition as an authorized user by means of access codes, passwords, and/or label checks.

6.5.2. Annually provide each file owner with a list of files belonging to his/her account number so that the owner can submit annual notices to the Information Practices Officer and instruct the Computer Center regarding changes to access codes, label checks, and permits for file release.

6.5.3. Develop written procedures governing physical release and programmed disclosure of automated files containing personal information. These procedures should include provisions for permanent and temporary permits, as well as the use of access codes and/or label checks.

6.5.4. Utilize other security measures as appropriate, such as encoding or decoding dates and cryptography.

6.5.5. Develop internal security procedures such as limiting use of access codes, label checks, and files to staff who have a need to know, and limiting physical access to areas of the Computer Center containing sensitive information.

6.5.6. Develop procedures for conducting periodic file inventories and reporting missing files containing personal information to the Information Practices Officer.

6.5.7. Provide new Computer Center staff with copies of procedures and obtain written acknowledgement that they have read and understood them. Periodic information practices refresher sessions will be held with current employees.

6.5.8. Develop an internal security manual delineating rules and procedures for physical and data security as well as for personal and confidential information practices.

7.0. PROCEDURES:

7.1. Annual Notice:

7.1.1. By April 1 of each year, the Director of Data Processing and Network Operations will provide the owners of automated files with a list of files belonging to their account numbers.

By May 1, the Information Practices Officer will send a request to all Record Custodians and Owners of Automated Files requesting changes, additions, or deletions to the Personal / Confidential Records Report Form currently on file for their records systems.

7.1.2. The Record Custodians and Owners of Automated Files will respond to the request for information by May 15.

7.1.3. The Information Practices Officer will file the required report with the Chancellor's Office by July 1.

7.2. Access and Photocopies:

7.2.1. Access procedures for student records and personnel records are detailed in the Administrative Procedures for those types of records. Individuals seeking access to other records to which they are entitled to inspect may submit a Request for Records Access form to the custodian of the record or appear in person during normal business hours to request access and complete the form. The individual requesting access will be asked to provide identification bearing a photograph and signature. The University will provide access to inspect and review records no later than thirty (30) days for active records and sixty (60) days for inactive records. In most instances the response will be provided in much less time than these maximum time limits.

7.2.2. If the individual requests copies of records on the Request for Photocopy form, the individual will pay ten (10) cents per page in cash, money order or cashier's check at the University Cashier's Office. Upon presenting a receipt for payment to the record custodian, copies of the records will be released.

7.3. Disclosure:

7.3.1. Disclosure procedures for student records and personnel records are detailed in the Administrative Procedure for those types of records. Individuals requesting disclosure of other types of records for which disclosure is permitted will sign a written consent. The consent will be maintained permanently with the record.

7.3.2. The record custodian will verify that the requesting individual has written permission to obtain information and is entitled to access. The record custodian will log all instances of disclosure on the disclosure log.

7.4. Amendment:

7.4.1. Detailed procedures for processing requests to amend student records and personnel records are found in the Administrative Procedures for those types of records. Individuals seeking to amend miscellaneous records will complete the Request to Amend Records form and submit the form to the record custodian.

7.4.2. The record custodian will make a determination with regard to amending the record within thirty (30) days following receipt of request. In the event that the request is denied, the individual may file a statement of reasonable length to become a part of the record.

7.4.3. In the event that the requesting individual challenges a refusal to amend the record, the matter will be reviewed by the Information Practices Officer and a response will be given to the individual within thirty (30) working days.

7.5. Violations--Individuals or department administrators will promptly report suspected violations of information practices or data security procedures to the Information Practices Officer.

8.0. APPENDICES:

8.1. Personal / Confidential Records Report, Form 694.

8.2. Rules of Conduct for University Employees Involved with Information Regarding Individuals.

8.3. Request for Records Access.

8.4. Request for Photocopy.

8.5. Request to Amend Record.

8.6. Disclosure Log.

8.7. Privacy Notice (Sample).

Appendix 8.2.

RULES OF CONDUCT FOR UNIVERSITY EMPLOYEES INVOLVED WITH INFORMATION REGARDING INDIVIDUALS

Employees shall:

1. Not disclose personal and confidential information relating to individuals to unauthorized persons or entities. The intentional disclosure of such information to such persons or agencies may be cause for disciplinary action, including dismissal.

2. Not seek out or use personal or confidential information relating to others for their own interest or advantage. The intentional violation of this rule may be cause for disciplinary action, including dismissal.

3. Take all necessary precautions to assure that proper administrative, technical, and physical safeguards are established and followed in order to protect the confidentiality of records containing personal information and to assure that such records are not disclosed to unauthorized individuals or entities.

4. Not require individuals to disclose personal information which is not necessary and relevant to the purposes of the campus or to the particular function for which the employee is responsible.

5. Make every reasonable effort to see that inquiries and requests relating to personal records of individuals are responded to quickly and without requiring the individual to unnecessarily repeat his or her inquiry to others.

Employees responsible for the collection, maintenance, use, and dissemination of information about individuals which relates to their personal life, including their employment and medical history, financial transactions, marital status and dependents, shall comply with the provisions of the State of California Information Practices Act.

6. Assist individuals who seek information pertaining to themselves in making their inquiries sufficiently specific and descriptive so as to facilitate locating the records.

7. Respond to inquiries from individuals, and requests from them to review, obtain copies of, amend, correct, or dispute their personal records in a courteous and businesslike manner, and in accordance with campus procedures for access and amendment of personal records developed in accordance with Sections 1798.30 through 1798.42 of the Information Practices Act.

I have read and understand the above rules of conduct.

_____Date_____

Employee Signature