MEMO TO: All University Offices  
FROM: Robert A. Kennelly, Vice President, Administration  
SUEJECT: Privacy and Personal Information Management  
Procedures for Records in the Custody of the  
Campus Computer Center  

The attached procedures covering Privacy and Personal Information Management Procedures for Records in the Custody of the Campus Computer Center have been developed by the Office of Institutional Studies in consultation with the Computer Center to implement Trustee policy resulting from the Information Practices Act of 1977 and the Family Education Rights and Privacy Act of 1974. They have been placed in effect as of July 1, 1978. Please insure that all staff members who are directly concerned with such records are provided with a copy.

If you need additional copies or have questions about the procedures please call Institutional Studies (X3655).

RAK: jd
Effective July 1, 1978, this campus has revised the procedures governing the use of automated files in the custody of the Campus Computer Center which contain personal or confidential information. These revised procedures are consistent with the Information Practices Act of 1977 (which has become Title 1.8 commencing with Section 1798 of Part 4 of Division 3 of the Civil Code of the State of California) and also with the Family Education Rights and Privacy Act of 1974 (20 U.S.C. 1232g), the regulations adopted thereunder (45 C.F.R. 99) and Section 24317 (SBL588 Roberti) of the California Education Code.

The following revised procedures pertain only to those automated files which are in the custody of the Campus Computer Center and concern the identification of personal files and their owners, the recognition of their authorized users, the programmed disclosure of such files, their physical release, the annual verification of authorized users and physical release permits, the maintenance of a file inventory, and general information security.

Identification of Files

Every file containing personal or confidential information which is maintained through the use of a computer or related peripheral equipment and which is in the custody of the Campus Computer Center is identified by owner. This includes all machine-readable files, whether on cards, tape or disk, with the exception of temporary working files created as intermediate steps in the production of reports or other files, when such working files are not retained for a period of more than one quarter. Such temporary working files are considered to be uses of the parent file or files from which they are created.

In most cases, the owner of a file is the owner of the system master file and is the individual or office responsible for the maintenance and update of the information contained therein. In those cases where two offices maintain information on a single master file, one office is designated as the owner (generally the office under whose account the file is created) and the other office is designated as a permanently authorized user.

The Campus Computer Center is responsible for the initial identification of all personal or confidential files maintained in its custody and for the initial assignment of such personal files to owners. The Campus Computer Center is also responsible for the creation and maintenance of an Owner and Authorized User File containing ownership and authorized user information on all such identified files. This Owner and Authorized User File is used to produce an annual listing of personal files by owner for owner verification and for the filing of record notices, and is used by the Campus Computer Center to verify the authorization for all requests to access personal files.

Recognition of Authorized File Users

Use of personal files is restricted to the file owners, to users who have received written authorization from the file owners, and to members of the CSUC
staff having direct line authority over the file owners. No other personnel may access any files containing personal or confidential information. The scheduling and running of all programs which access personal files is the responsibility of the Campus Computer Center. No request to access personal or confidential files will be honored unless the Campus Computer Center has verified that the request comes from an authorized user of the affected personal files.

For all programs which access personal files and which are regularly scheduled in support of University operations, an annual verification made to determine that the requesting office is either the owner or an authorized user of all personal files accessed and that the distribution list maintained in the Campus Computer Center for all output produced by these programs has been reviewed and authorized by the requesting office. Such routine support programs are entered onto the master operation schedule for the Campus Computer Center and do not require a separate Request for Data Processing Services or Supplies form (L-1-900-67) before each such scheduled run. Whenever the output from such programs contains personal or confidential information, release of such output is made only to the requesting office and to those other individuals or offices which have been authorized to receive the information, as indicated on the Report Distribution List. Delivery of all such output containing personal or confidential information is acknowledged by the signature of the authorized individual accepting delivery.

For all programs accessing personal or confidential files which are not designated as routine support programs, a Request for Data Processing Service and Supplies form (L-1-900-67) must be submitted to the Campus Computer Center. The Campus Computer Center verifies that the requesting office is the owner or permanent authorized user of all personal files to be accessed. If the requesting office or individual is not the owner or permanently authorized user of all affected personal files, it is the responsibility of the requester to obtain approval for the temporary use of such files by obtaining the signature of each file owner on the indicated line of the request form. If the output from such programs contains personal information, then it is delivered only to the approved requester with delivery acknowledged by signature.

User-supplied programs which access personal or confidential files maintained in the custody of the Campus Computer Center will not be run. However, the Campus Computer Center will extract requested data from personal or confidential files in its custody for use with a user-supplied program if the creation of such an extracted file is authorized by the accessed file owners. If the resulting output contains personal information, then delivery of such output will be made only to the approved requester with receipt acknowledged by signature.

New Requests for Programmed Access of Personal or Confidential Files

Whenever a new programming request involves the use of personal or confidential files, it is the responsibility of the Campus Computer Center to verify that the requesting office or individual owns or is permanently authorized to access the desired files. Where such authorization has not been made, the
programming staff, in conjunction with the requesting office or individual, meets with each affected file owner to discuss the project and to obtain either permanent or temporary authorization to access the files. Permanent authorization is entered on the Owner and Authorized User File. Temporary authorization requires the signature of the file owner on the run request form (L-1-900-67) each time the program is run. No program may be tested, installed, or run until authorization to use all accessed personal files is obtained from the affected file owners.

**Physical Release of Personal or Confidential Files**

All personal or confidential files in the custody of the Campus Computer Center are released only to the custody of the file owner unless permission to release a file to other than the file owner is supplied to the Campus Computer Center by the file owner on the Authorization for the Release of Personal or Confidential Files form supplied by the Campus Computer Center. Such permission must state the name of the individual or department to whom the file is to be released, all limitations on the use, copying, and transfer of information from the file, and the length of time for which the permission is to be in effect. In some cases, as when files are transmitted off-campus to be microfiched or sent to the Chancellor's Office, permanent authorization is appropriate. In most cases, however, permission to release a personal file will be temporary, for one occurrence only.

In order to avoid the possibility of unauthorized modification of files, the release of all personal files to other than the file owner is in the form of a duplicate of the requested file. When the released file is returned, it is not reentered into the Campus Computer Center operations, but is scratched or destroyed in the manner appropriate for the release of working files of a similar type.

**Annual Review of Authorized Users and Release Permits**

While it is the responsibility of the file owners to prepare and submit record notices to the Chancellor's Office for all automated files containing personal or confidential information, the Campus Computer Center assists this effort by producing and distributing to each owner a list of all owned files and their authorized users and any physical release authorizations on file. Prior to the filing of the record notices, the Campus Computer Center personnel and the Information Practices Officer meet with each file owner to review the list of authorized users and any permits for physical release and to make any necessary additions, corrections or deletions. One updated copy of this verification list is retained by the file owner and a duplicate, signed by the owner, is used to update the Owner and Authorized User File. The signed verification list is retained in the Campus Computer Center until the next annual verification has been completed.
Inventory of Files

The Campus Computer Center maintains an inventory of all files, including those which contain personal or confidential information. Should any file be missing, the circumstances concerning its loss are carefully investigated. In most cases, the loss of a file is actually the loss of information resulting from the re-use of a tape or disk which contained information which should have been retained. The Campus Computer Center (in conjunction with the file owner) maintains sufficient file duplication to provide for the reconstruction of otherwise irreplaceable data files in the event of such a loss of information.

In any case where files containing personal or confidential information are discovered to be physically missing from the Campus Computer Center (an actual loss of a tape, disk, or card deck, rather than loss of information as a result of reading new information over information which should have been retained), the circumstances relating to the missing files shall be reported to the Information Practices Officer for further investigation. The Information Practices Officer shall convey the results of any such investigation to the Vice President, Administration, the Director of the Campus Computer Center and the file owner for further action as indicated.

Information Security

It is the policy of the campus that personal or confidential data is entered onto automated files only on a need-to-know basis and available only to those with a verified need to access the information. Whenever possible, information, reports, or files extracted from personal files do not include an individual identifier, unless such individual identifier is necessary for the use of the information, reports, or files.

All tapes and disks in the custody of the Campus Computer Center are externally and internally labeled, and programs which access personal files include label checks. A log of all programs run is maintained for all operation for both accounting and information security uses. Further, access to the area in which files containing personal or confidential information are stored is limited to personnel whose duties require their presence in the area and to authorized escorted visitors.

All employees of the Campus Computer Center will be given copies of these procedures and shall acknowledge in writing that they have read and understood them. In addition, annual information sessions are held by the Information Security Officer to review current employee understanding of existing and new procedures.

These procedures, in conjunction with the Campus Information Security Manual, delineate the rules and procedures for physical and data security as well as for personal information management practices. All users and employees of the Campus Computer Center will be periodically informed regarding the civil penalties and dismissal possibilities for privacy intrusion resulting from a failure to observe these rules and procedures.