

# UC Davis Policy and Procedure Manual

## Chapter 310, Communications and Technology

### Section 24, Electronic Communications—Privacy and Access

Date: 5/9/06

Supersedes: Section 310-16, 10/5/04

Responsible Department: Information and Educational Technology

Source Document: University of California Electronic Communications Policy

---

*Exhibit A, Request to Inspect, Monitor, or Disclose Electronic Records—Access with Consent*

*Exhibit B, Request to Inspect or Disclose Electronic Records—Access Without Consent*

#### I. Purpose

This section provides UC Davis (UCD) implementing procedures for the privacy and disclosure of Electronic Communications (EC) records. The UC and UCD EC policies apply to all EC resources owned by the University, provided by the University through contracts and other agreements; users and uses of University EC resources; and all EC records in the possession of University employees or other users of University EC resources. See also Section 310-23, Electronic Communications—Allowable Use.

#### II. Definitions

- A. Authorizing official—at UCD, the authorizing officials are the Provost & Executive Vice Chancellor for academic appointee accounts, the Vice Chancellor—Student Affairs for student accounts, the Hospital Director for UCDHS nonacademic accounts, and the Vice Chancellor—Administration for staff, public users, and others. In the case of personal or conflicting interest, the authorizing official shall recuse himself or herself and the Chancellor shall designate an alternate official.
- B. Other terms used in this policy are defined in Section 310-23 and in the UC EC policy.

#### III. Policy

- A. The University recognizes that the principles of academic freedom, shared governance, and freedom of speech hold important implications for the use of electronic communications and respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations, while seeking to ensure that University administrative records are accessible for the conduct of University business.
- B. University employees are prohibited from seeking out, using, or disclosing personal information in electronic communications without authorization. Employees must take necessary precautions to protect the confidentiality of personal information encountered either in the performance of their duties or otherwise.

#### IV. Privacy and Access

- A. Users' electronic communications records shall not be examined or disclosed without the holder's consent except under the following limited circumstances:
  - 1. When required by and consistent with law.
  - 2. When there is substantiated reason to believe that violations of the law or University policies have taken place.

3. When there are compelling circumstances that preclude the holder's consent.
4. When there are time-dependent, critical operational circumstances.

See V.B, below for procedures to access records without consent.

- B. Privacy protections. Federal and State laws provide privacy protections for certain personal information, student information, electronically gathered data, and telephone conversations. (See References, below, for specific policies addressing these protections).
- C. Privacy limits
  1. Public records. EC records pertaining to the business of the University, whether or not created or recorded on University equipment, are University records and subject to disclosure under the California Public Records Act.
  2. System monitoring. During the performance of their duties, system administrators regularly monitor transmissions for the purpose of ensuring the proper functioning, reliability, and security of University EC resources and services. During this process, they may observe certain transactional information and the contents of electronic communications. Except as provided elsewhere in this policy or by law, system administrators are not permitted to seek out the contents or transactional information where not germane to the foregoing purposes, or disclose or otherwise use what they have observed. System monitoring is limited to the least amount of perusal required. If in the course of their duties, system administrators inadvertently discover or suspect improper activity in violation of law or policy, they shall report such incidents, consistent with University policy (see Section 380-17).
- D. Individuals who have been granted access to EC records:
  1. Must not use the grant of access to obtain records other than those required to continue University business in the holder's absence.
  2. Must limit their inspection of records to the least perusal of contents and the least action necessary to obtain the needed records.
  3. May seek out, use, or disclose personal information contained in the records for University business only.
  4. Must not violate the UCD Acceptable Use Policy regarding use of false identity.
  5. Must take all necessary steps to protect the access and/or account from unauthorized use.

## **V. Procedures**

- A. Access with consent

Exhibit A shall be used to track compliance with this policy. Holders may not be compelled to consent to allow others to access their electronic communications, however, the department may use the provisions on access without consent should the holder choose not to allow access

B. Access without consent

1. If necessary to prevent destruction or tampering with records, a service restriction may be made as described in 310-23.
2. The requestor shall complete Exhibit B and send it to the user's department head or to the Security Coordinator. If the request is the result of a court order, the request shall be sent to the Security Coordinator.
3. The department head or Security Coordinator shall determine if the request is consistent with the provisions of UC EC policy, IV.B.
4. The department head or Security Coordinator shall send Exhibit B to Campus Counsel.
5. Campus Counsel reviews the request and sends it to the authorizing official.
6. The authorizing official must seek the advice of Campus Counsel prior to any action involving records stored on equipment not owned of housed by the University; whose content is protected by FERPA; when the holder is not going to be notified of the access; or upon receipt of legal documents, such as search warrants, subpoena, or subpoena duces tecum, demanding access to information.
7. If the holder is a member of the faculty as defined in APM Section 110-4(14), the Provost and Executive Vice Chancellor shall consult in writing with the Chair of the Academic Senate. The time period allowed for consultation shall be specified by the Provost and Executive Vice Chancellor, and shall not exceed 5 working days.
8. If the authorizing official approves the request, the department head shall present Exhibit B to the appropriate system administrator.
9. The system administrator shall arrange for the requested electronic records to be accessed, providing only the relevant records, if any, to the requestor. The system administrator shall protect the account from unauthorized use or access.
10. At the earliest possible opportunity that is lawful to do so and consistent with other University policy, the holder shall be notified of the action taken and the reason for it.

C. Procedures for emergency circumstances

In emergency circumstances as defined in the UC EC policy, records may be inspected, monitored, or disclosed without the prior consent of the authorizing official. The following procedures shall be used in emergency circumstances:

1. The system administrator shall obtain the authorization of the department head, access the records, and notify the authorizing official.
2. The department head, without delay, shall complete Exhibit B and follow the procedures provided in V.B, above.
3. If the approval of the authorizing official is not subsequently given, the department head shall take measures to restore the situation as closely as possible to that existing before action was taken.

D. Recourse to access without consent

The holder whose records were accessed without consent may appeal the decision to the Chancellor within 30 days of the notification. If the Chancellor determines that access should not have taken place, all individuals who participated in the access shall take measures to restore the situation as closely as possible to that existing before action was taken.

**VI. References and Related Policies**

A. Office of the President: University of California Electronic Communications Policy.

B. UC Davis Policy and Procedure Manual:

1. Section 310-10, Telecommunications Services.
2. Section 310-23, Electronic Communications—Allowable Use.
3. Section 320-10, Records Management Program.
4. Section 320-20, Privacy and Access to Information.
5. Section 320-21, Disclosure of Information from Student Records.
6. Section 380-17, Improper Governmental Activities.

C. Academic Personnel Manual:

1. Section 158, Rights of Academic Employees, Including Rights Regarding Records.
2. Section 160, Academic Personnel Records/Maintenance of, Access to, and Opportunity to Request Amendment of.

D. UC Business and Finance Bulletins:

1. IS-3, Electronic Information Security.
2. RMP-7, Privacy of and Access to Information Responsibilities.
3. RMP-8, Legal Requirements on Privacy of and Access to Information.

E. State of California Statutes:

1. Information Practices Act of 1977 (Civil Code Section 1798 et seq.).
2. Public Records Act (Government Code Section 6250 et seq.).
3. Government Code Section 11015.5.
4. Penal Code Section 502 and 1523 et seq.

F. Federal statutes and regulations:

1. Electronic Communications Privacy Act of 1986 (U.S. Code Title 18, Section 2510 et seq.).
2. Family Education Rights and Privacy Act of 1974 (U.S. Code Title 20, Section 1232g).