

Electronic Communications Policy

Attachment 2 Implementation Guidelines

University of California
Office of the President

Issued November 17, 2000
Updated January 14, 2005

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PURPOSE	1
B.	CAMPUS RESPONSIBILITIES	1
II.	ALLOWABLE USE.....	2
A.	ALLOWABLE USERS	2
B.	ALLOWABLE USES	3
C.	ACCESS RESTRICTION	5
D.	USE OF SPECIFIC SERVICES	5
III.	PRIVACY AND CONFIDENTIALITY	6
A.	ACCESS WITHOUT CONSENT	6
B.	PRIVACY PROTECTIONS AND LIMITS	8
C.	PRIVACY OF SPECIFIC SERVICES	10

I. INTRODUCTION

A. *PURPOSE*

The purpose of these Implementation Guidelines is to provide guidance to campuses on implementation of the Electronic Communications Policy.

B. *CAMPUS RESPONSIBILITIES*

Campuses shall develop guidelines and procedures for the following:

- a. Each Chancellor shall establish guidelines as to who may use the electronic communications resources under that Chancellor's jurisdiction, consistent with provisions of Policy Section III.C, Allowable Users.
- b. Each Chancellor shall establish regulations and procedures on actions to be taken once a user's affiliation with the campus is terminated. In particular, the campus may elect to terminate the individual's access, redirect electronic communications, or continue the access, subject to provisions of Policy Section III.C, Allowable Users, and consistent with Business and Finance Bulletin IS-3, Electronic Information Security.
- c. Each Chancellor shall establish guidelines and procedures for:
 - Restricting or denying the use of University electronic communications resources in accordance with Policy Section III.E, Access Restriction;
 - Authorization, advice, notification, and recourse as required by Policy Section IV.B, Access Without Consent; and
 - Response to user requests for information about the back-up of electronic communications, as required by Policy Section IV.C, Privacy Protections and Limits.
- d. Each Chancellor shall designate the appropriate Vice Chancellor(s) to authorize action pursuant to Policy Sections III.D, Access Restriction, and IV.B, Access Without Consent. The authority for access without consent may not be further re-delegated.

The designated Vice Chancellor is responsible for recusing him/herself in the event of personal or conflicting interests in a specific situation regarding Access Restriction or Access Without Consent. Each Chancellor shall

designate a temporary alternate Vice Chancellor in the event of such conflicts of interest.

- e. Each Chancellor shall establish procedures for responding promptly to allegations regarding copyright infringement, sexual or other forms of harassment, defamation, and other violations arising from electronic communications where the University might be responsible for mitigation (see Electronic Communications Policy, Section III.E, Access Restriction).
- f. Each Chancellor may establish campus guidelines covering:
 - Procedures for reimbursement of incremental costs incurred for incidental personal use of University electronic communications resources (see Electronic Communications Policy Section III.D, Allowable Uses);
 - Establishment of web pages, mailing list systems, newsgroups and bulletin boards for personal use on University electronic communications resources;
 - Procedures for identifying official University web pages; and
 - Methods for billing residence hall telephone systems.
- g. In accordance with the policies and procedures in the University's Policy Applying to the Disclosure of Information from Student Records (Sections 130-134 of the Policies Applying to Campus Activities, Organizations, and Students), each Chancellor shall designate the categories of personally identifiable information about a student that are public and shall establish procedures by which individual students may request that the campus not make public their electronic mail addresses and telephone numbers (see Electronic Communications Policy Section IV.C.1, Privacy Protections).
- h. Each Chancellor may establish additional procedures that further refine and conform with this Policy.
- i. For purposes of this Policy, the Office of the President shall be regarded as a campus with respect to its own internal operations.

II. ALLOWABLE USE

A. ALLOWABLE USERS

Chancellors shall establish guidelines as to who may use the electronic communications resources under their jurisdiction. Campus guidelines should reflect the following general principles of the Electronic Communications Policy:

- Section III.C identifies members of the University community as the intended users of University electronic communications resources;
- Section III.D.1, Purpose, requires that use of University electronic communications resources be in support of the University's mission;
- Section III.D.2, Non-Competition, requires that campuses not compete with private electronic communications providers by providing services to users outside the University except where such services are unique or where providing them demonstrably supports the University's mission;
- Section III.E, Access Restriction, declares that access to University electronic communications resources is a privilege rather than a right;
- Section III.E, Access Restriction, allows for restriction of access under specified circumstances regardless of the normal conditions of use established by the manager of the individual electronic communications resource.

Campus guidelines should begin from the assumption that the level of access granted University Users of electronic communications resources terminates when the user's affiliation with the University ends. Exceptions may be made when extending this level of access serves the University's mission and does not constitute competition with commercial service providers.

B. ALLOWABLE USES

- 1. Representation.** When an electronic communication inaccurately gives the impression that the author represents the University, the communication must include an explicit disclaimer. Campus guidelines should provide means of meeting this requirement concerning implied representation. Among other alternatives, they may: i) provide specifications for a context that makes a disclaimer unnecessary for a particular electronic communications service; ii) provide for a common disclaimer that can be shared by users of an electronic communication service; or iii) suggest the wording of a disclaimer to be included by the author, e.g. "These statements are my own, not those of the Regents of the University of California."
- 2. Endorsements.** When an electronic communication might give the impression that the author's endorsement represents an endorsement by the University, the communication must include an explicit disclaimer. Campus guidelines should provide means of meeting this requirement concerning implied endorsements. Among other alternatives, they may: i) provide specifications for a context that makes a disclaimer unnecessary for a particular electronic communications service; ii) provide for a common disclaimer that can be shared by users of an electronic communication service; or iii) suggest the wording of a disclaimer to be included by the author, e.g. "References or pointers to non-University entities do not represent endorsement by the Regents of the University of California."

Campus guidelines shall not restrict faculty evaluation of educational materials in the context of teaching and research.

- 3. Anonymity.** Campus guidelines may restrict the circumstances under which pseudonyms and anonymity are permitted in electronic communications. However, local guidelines must not preclude the use of anonymous electronic communications for the purpose of whistleblowing, in conformance with ~~Business and Finance Bulletin G-29, Procedures for Investigating Misuse of University Resources~~ **the Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (the "Whistleblower Policy")**.

Public communications such as web publication and broadcast transmissions may not be anonymous (see Use of Specific Services below).

- 4. Interference.** Campus guidelines should identify examples of behaviors that are likely to interfere with the operation of University electronic communications resources so users can, in good faith, avoid them. Guidelines should clarify that additional behaviors may also prove to be disruptive, since technological advances may lead to new abuses of electronic communications resources. Guidelines should also distinguish between behaviors that are purposeful and those that cause unintended disruption of services.
- 5. Personal Use.** Campus implementing guidelines may specify terms and conditions for the personal use of specific electronic communications services, consistent with the provisions for personal use in Policy Section III.D.8.

Operators of electronic communications systems and services may (consistent with Policy Sections III.D.7, Interference, and V.A and B, Security) proscribe specific personal use practices (see Interference above). In addition, operators may restrict access, according to established campus procedures, to electronic communications resources for personal use on an ad hoc or long term basis as described in the Policy, Section III.E, Access Restriction.

Users should be encouraged to avoid noticeable incremental charges to the University for personal use of University facilities by employing telephone cards, private email accounts, and other mechanisms to charge such costs to personal accounts. When personal use causes noticeable incremental costs to the University, users shall reimburse the University following campus procedures and guidelines (see Electronic Communications Policy Section III.D.8, Personal Use and Responsibilities above).

- 6. Accessibility.** Operators of University electronic communications resources should coordinate with campus officers responsible for implementation of the Americans with Disabilities Act to ensure that persons with disabilities have access to those resources.

7. **Intellectual Property.** As required by the Digital Millennium Copyright Act, campuses should provide users with information regarding copyright laws and should refer them to the University's Guidelines for Compliance with the Online Service Provider Provisions of the Digital Millennium Copyright Act (see Electronic Communications Policy Section III.D.10).

C. ACCESS RESTRICTION

The Policy does not require the same high level authorization for restricting users' access to electronic communications resources as it does for nonconsensual access by others to electronic communications records without the consent of the holder. However, campus implementing guidelines must identify the procedures for restricting access when the authorization of a Vice Chancellor is not required. Such procedures must conform to the requirements of Policy Section III.E, Access Restriction, and be applicable on a consistent basis campuswide. Electronic communications resource providers may, nonetheless, restrict access on a temporary basis as needed in Emergency Circumstances and Compelling Circumstances (see Electronic Communications Policy Section IV.B.2, Emergency Circumstances, and Appendix A, Definitions) in order to control an emergency or prevent damage or loss.

D. USE OF SPECIFIC SERVICES

1. Web Pages

Campus guidelines shall ensure that the following requirements for publishing web pages are met:

- a. **Identification.** Web pages shall not be posted anonymously at addresses within a University domain (i.e., campus.edu). Campus guidelines may establish local standards for identifying the University unit, sub-unit, program, or individual responsible for the page.
- b. **Official University Web Pages.** The Chancellor shall determine what rules to apply to web pages in order to comply with provisions of Policy Sections III.D. 4 and 5, Representation and Endorsement. For this purpose, the Chancellor may designate certain web pages as official University web pages. Conversely, the Chancellor may designate mechanisms for identifying personal web pages that do not represent the University. Any identification used to denote official web pages must not be used for other web pages.

- c. **Personal Web Pages.** The establishment of personal web pages is subject to campus approval (see Personal Use, above). When personal web pages are permitted, campus guidelines should specify the conditions under which personal web pages are permitted. In addition, campus guidelines should establish local standards that will enable users to recognize that the page represents the individual rather than the University (see Representation and Endorsements, above).

2. Radio Frequency Stations

- a. **Station Licenses.** Operation of radio frequency stations (including television, radio, auxiliary broadcast facilities, maritime, aeronautical, land mobile, satellite, microwave, and paging) requires Federal Communications Commission licensing. Campuses shall apply for such licenses through the Office of the Associate Vice President, Information Resources and Communications.
- b. **Radio Frequency Interference.** Users of telecommunications radio frequency transmitters and receivers shall operate such equipment in compliance with regulations of the Federal Communications Commission. In particular, users shall not interfere with other station operators or other users on the same station, regardless of whether such operators or users are affiliated with the University.

III. PRIVACY AND CONFIDENTIALITY

A. ACCESS WITHOUT CONSENT

Each Chancellor shall establish guidelines and procedures for authorization, advice, notification, and recourse in cases of nonconsensual access to electronic communications (see Responsibilities, above).

1. **Authorization.** Campus procedures for authorization to access electronic communications without consent shall ~~ensure that~~ **include** the following requirements ~~are met~~:
 - ~~Except in emergency circumstances,~~ **Requests for nonconsensual access must be submitted in writing except in emergency circumstances. In accordance with Policy Section IV.B.2, Emergency Circumstances, actions must be limited to the least perusal of contents and the least action necessary to resolve the emergency. Appropriate written authorization must subsequently be sought without delay.**

- ~~University Counsel's~~ **Advice of campus counsel or an attorney in the Office of General Counsel** shall be sought prior to authorization of nonconsensual access. **Counsel's advice shall be sought in the event of receipt of legal documents demanding information, such as subpoena duces tecum, subpoena, or search warrant, in accordance with Policy Section IV.B, Access without Consent and RMP-10, Instructions for Responding to Subpoena, and campus implementing procedures.**
- 2. Procedures concerning faculty.** Chancellors shall confer with their respective Divisional Senate to establish procedures for nonconsensual access to electronic communications where the inspection, monitoring, or disclosure involves electronic communications held by faculty.
 - 3. 2. Notification.** Advice of Counsel shall be sought in determining whether there is reason not to notify an individual that his or her electronic communications have been accessed without consent.
 - 4. 3. Annual Report.** Each Chancellor shall annually report to the Office of Information Resources and Communications in the Office of the President the number of cases of nonconsensual access to electronic communications that have taken place. The annual report will identify the:
 - Number of requests for nonconsensual access,
 - Number of requests granted on emergency basis,
 - Number of requests granted after prior approval,
 - Number of requests denied, and
 - Reasons for requests: (i) Required by and consistent with law, (ii) Substantiated reason to believe that violations of law or University policies have taken place, (iii) Compelling circumstances, and/or (iv) Time-dependent, critical operational circumstances.

Annual reports shall consist of summary numbers with no information about individual cases, and shall be posted on the web so the data will be available to the University community and the public. **Requests that result from search warrants, subpoenas, subpoenas duces tecum or other court orders shall be included in annual reports.**

- 5. 4. Recourse.** Campus procedures for appeal of decisions regarding nonconsensual access to electronic communications (whether under normal authorization procedures or Emergency Circumstances) should whenever possible use existing mechanisms for faculty, staff, and student actions and appeals.

B. PRIVACY PROTECTIONS AND LIMITS

1. **Personal Information.** A written release should be obtained prior to posting, broadcasting, or distributing an individual's picture or statement, except in cases of news reporting.
2. **Student Information.** Campus guidelines should clarify what student information may and may not be released, consistent with Policy Section IV.C.1.b, Student Information, and Responsibilities I.B.g. above.
3. **Electronically Gathered Data.** When a University electronic communications service automatically collects information about a user (for instance, through cookies and banner ads), notice to that effect should be posted at the beginning of the transaction and should indicate what information will be collected and how it will be used. Ideally, users should be allowed to terminate the transaction at that point without leaving data behind.
4. **Unavoidable Inspection.** Campus guidelines shall ensure that University personnel who operate and support electronic communications resources **understand and** comply with the provisions of Policy Section IV.C.2.c, Unavoidable Inspection, regarding the conditions under which they may observe the contents of electronic communications **or transactional information**. This section of the Policy also requires that they not disclose the contents of communications they have observed, **except as required by law or policy**.

For purposes of the Electronic Communications Policy, automated inspection of electronic communications in order to protect the integrity of University electronic communication resources does not constitute nonconsensual access (see Electronic Communications Policy Sections III.D.7, Interference, IV.C.2.c, Unavoidable Inspection, and V.A., Security).

5. Access to University Administrative Records.

Consistent with Policy Section IV.A, Introduction, campus guidelines shall include procedures to ensure that University administrative records are accessible for the conduct of the University's business.

- a) **Absences.** In order to reduce the need to access an employee's email in the event of absence, campuses may use techniques or procedures to minimize the need to gain access without consent. Following are some practices that campuses may implement.
 - **Workgroup accounts.** Establish common workgroup accounts for department-related business so essential departmental business electronic communications are accessible to all workgroup members.

- *“Absence” messages.* Include in procedures the requirement that absence messages be installed to indicate the period of time of absence and alternate contact information.
 - *Email forwarding.* Use email forwarding capabilities, if available, so that during planned absences electronic communications will be forwarded to authorized individual(s).
 - *Autoforwarding with Filtering.* Set filters to forward selected electronic communications to relevant staff in the holder’s absence.
 - *Mailing lists.* Establish mailing lists so that all subscribers receive a copy of any messages posted to the list.
 - *Shared files.* Establish files server capability to store and access documents in support of business operations. Authorization and access procedures must be clearly documented.
- b) Separated Employees. Appropriate campus guidelines shall include recommendations for exit procedures that include clear instructions regarding the disposition of employee electronic communications records subsequent to the employee’s separation from the University. Employees shall be informed of these procedures upon employment.

Exit procedures shall include:

- conditions governing departmental access to the employee’s electronic communications subsequent to the employee’s termination.
- instructions regarding disposition of personal electronic communications records, such as whether they should be deleted or transmitted to other personal email accounts or other personal media.
- instructions if absence message must be installed, indicating termination date and contact information for departmental business.
- date at which time the account will be terminated and not accessible to the former employee.

Exit procedures shall identify intended reuse or disposal of electronic communication resources and the electronic communications records stored on those resources upon employee separation.

In cases of involuntary separation, exit procedures shall include standard notification to be sent to employees. Such notification shall include:

- conditions governing employee’s access to electronic communications resources during period of separation, including any arrangements to permit employee temporary access to obtain copies of personal electronic communications.
- date when access to electronic communications will terminate.

- c) Death. Disposition of electronic communications of deceased individuals shall follow campus guidelines or protocols. In the absence of guidelines or protocols, advice of legal counsel shall be sought if requests for access to a former holder’s electronic communications records are received.

C. PRIVACY OF SPECIFIC SERVICES

- 1. Telephone Transaction Records.** Accounting procedures require billing records to be provided to University units and sub-units for review. Telephone transaction records document the use of University telephone equipment, including the number called and the time and length of the call. University units should advise employees who use University telephones for personal or other purposes that supervisors have access to records of all calls made from University telephones assigned to their use and that such records may be used for administrative purposes.