

Electronic Communications Policy

University of California
Office of the President

Issued November 17, 2000
Revised August 18, 2005

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	GENERAL PROVISIONS.....	2
	A. PURPOSE	2
	B. SCOPE	2
	C. DEFINITIONS.....	3
	D. RESPONSIBILITIES.....	3
	E. VIOLATIONS OF LAW AND POLICY	4
III.	ALLOWABLE USE.....	5
	A. INTRODUCTION	5
	B. OWNERSHIP	5
	C. ALLOWABLE USERS.....	6
	D. ALLOWABLE USES	6
	E. ACCESS RESTRICTION.....	9
IV.	PRIVACY AND CONFIDENTIALITY	10
	A. INTRODUCTION	10
	B. ACCESS WITHOUT CONSENT.....	10
	C. PRIVACY PROTECTIONS AND LIMITS.....	12
V.	SECURITY.....	15
	A. INTRODUCTION	15
	B. SECURITY PRACTICES.....	15
	C. INTEGRITY.....	15
	D. AUTHENTICATION	16
	E. AUTHORIZATION.....	16
	F. ENCRYPTION	16
	G. RECOVERY	16
	H. AUDIT	16
VI.	RETENTION AND DISPOSITION.....	17
	A. RETENTION	17
	B. DISPOSITION.....	17
	C. BACK-UP	17
	APPENDIX A: DEFINITIONS.....	18
	APPENDIX B: REFERENCES	21
	APPENDIX C: POLICIES RELATING TO ACCESS WITHOUT CONSENT	23
	SUPPORTING DOCUMENTS.....	24
	Attachment 1 User Advisories	
	Attachment 2 Implementation Guidelines	

I. INTRODUCTION

The University of California encourages the use of electronic communications to share information and knowledge in support of the University's mission of education, research and public service and to conduct the University's business. To this end, the University supports and provides interactive electronic communications services and facilities for telecommunications, mail, publishing, and broadcasting.

Recognizing the convergence of technologies based on voice, video, and data networks, as Presidential Policy [<http://www.ucop.edu/ucophome/coordrev/policy/>], the University of California Electronic Communications Policy establishes principles, rules, and procedures applying to all members of the University community to specifically address issues particular to the use of electronic communications. It clarifies the applicability of law to electronic communications and references other University guidelines to ensure consistent application of the Electronic Communications Policy on all University campuses (see Appendix B, References).

II. GENERAL PROVISIONS

A. PURPOSE

The purposes of this Policy are to:

- Establish policy on privacy, confidentiality, and security in electronic communications;
- Ensure that University electronic communications resources are used for purposes appropriate to the University's mission;
- Inform the University community about the applicability of laws and University policies to electronic communications;
- Ensure that electronic communications resources are used in compliance with those laws and University policies; and
- Prevent disruptions to and misuse of University electronic communications resources, services, and activities.

B. SCOPE

This Policy applies to:

- All electronic communications resources owned or managed by the University;
- All electronic communications resources provided by the University through contracts and other agreements with the University;
- All users and uses of University electronic communications resources; and
- All University electronic communications records in the possession of University employees or of other users of electronic communications resources provided by the University.

This Policy does not apply to electronic communications resources of the Department of Energy Laboratories managed by the University, or to users of such electronic communications resources who are employees and agents of those Laboratories. The Policy does apply to University users (as defined here) of the DOE Laboratories' electronic communications resources, to the extent that the provisions of the Policy are not superseded by those of DOE Laboratories managed by the University.

This Policy applies to the contents of electronic communications, and to the electronic attachments and transactional information associated with such communications.

This Policy applies only to electronic communications records in electronic form. The Policy does not apply to printed copies of electronic communications records or printed copies of transactional information. Electronic communications records in either printed or electronic form are subject to federal and state laws as well as University records management policies, including their provisions regarding retention and disclosure (see State of California Statutes, Federal Statutes and Regulations, and Business and Finance Bulletins in the Records Management and Privacy (RMP) series listed in Appendix B, References).

C. DEFINITIONS

The following terms used in this Policy are defined in Appendix A, Definitions. Knowledge of these definitions is important to an understanding of this Policy.

- Compelling Circumstances
- Electronic Communications
- Electronic Communications Resources
- Electronic Communications Records
- Electronic Communications Service Provider
- Electronic Communications Systems or Services
- Emergency Circumstances
- Faculty
- Holder of an Electronic Communications Record or Electronic Communications Holder
- Possession of Electronic Communications Record
- Public Record
- Substantiated Reason
- Time-dependent, Critical Operational Circumstances
- Transactional Information
- University Administrative Record
- University Electronic Communications Record
- University Electronic Communications Systems or Services
- Use of Electronic Communications Services

D. RESPONSIBILITIES

1. **Policy.** This Policy is issued by the President of the University of California. The Associate Vice President, Information Resources and Communications (IR&C) in the Office of the President is responsible for maintenance of this Policy.

2. **Implementation.** Each Chancellor, and for the Office of the President, the Senior Vice President, Business and Finance, shall designate a coordinator to administer the Policy. In consultation with faculty, students, and staff, the designated coordinator shall develop, maintain, and publish specific procedures and practices that implement this Policy. Campus procedures shall include information on accessibility of student information, authorized users, procedures for restricting or denying use of its electronic communications services, adjudication of complaints, network monitoring practices, and other matters as described in Attachment 2, Implementation Guidelines. IR&C shall facilitate regular communication among campus coordinators to address consistency in campus implementing procedures.
3. **Informational Material.** Campuses shall provide users of University electronic communications resources with instructional material based on this Policy and on their own campus implementation guidelines.

E. VIOLATIONS OF LAW AND POLICY

1. **Law.** Federal and state law prohibit the theft or abuse of computers and other electronic resources such as electronic communications resources, systems, and services. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of electronic communications resources, systems, and services. The law classifies certain types of offenses as felonies (see Appendix B, References).
2. **University Disciplinary Actions.** University policy prohibits the use of University property for illegal purposes and for purposes not in support of the mission of the University. In addition to legal sanctions, violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to University policies and collective bargaining agreements. Further information on permitted and prohibited uses is given in Section III, Allowable Use.

III. ALLOWABLE USE

A. INTRODUCTION

The University encourages the use of electronic communications resources and makes them widely available to the University community. Nonetheless, the use of electronic communications resources is limited by restrictions that apply to all University property and by constraints necessary for the reliable operation of electronic communications systems and services. The University reserves the right to deny use of its electronic communications services when necessary to satisfy these restrictions and constraints.

In general, the University cannot and does not wish to be the arbiter of the contents of electronic communications. Neither can the University always protect users from receiving electronic messages they might find offensive.

B. OWNERSHIP

This Policy does not address the ownership of intellectual property stored on or transmitted through University electronic communications resources. Ownership of intellectual property is governed by law, the University of California Policy on Copyright Ownership (1992) and the 2003 Policy on Ownership of Course Materials, Academic Personnel Policy 020, Special Services to Individuals and Organizations (Regulation 4), and other University policies and contracts (see Appendix B, References).

University policy issued by Vice President Bolton on October 31, 1969 and reiterated in Business and Finance Bulletin RMP-1, University Records Management Program (see Appendix B, References) assigns the ownership of the administrative records of the University to The Regents of the University of California. This applies whether such records are in paper, digital, or other format. Electronic communications records pertaining to the administrative business of the University are considered public records (see Appendix A, Definitions), whether or not the University owns the electronic communications resources, systems or services used to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, print, or otherwise record them. Other records, although not owned by The Regents, nevertheless may be subject to disclosure as public records under the California Public Records Act if they pertain to the business of the University.

University electronic communications resources, systems and services are the property of The Regents of the University of California. These include all components of the electronic communications physical infrastructure and any

electronic communications address, number, account, or other identifier associated with the University or any unit of the University or assigned by the University to individuals, units, or functions.

C. ALLOWABLE USERS

- 1. University Users.** University students, faculty, staff, and others affiliated with the University (including those in program, contract, or license relationships with the University) may, as authorized by the Chancellor, be eligible to use University electronic communications resources and services for purposes in accordance with Sections III.D, Allowable Use.
- 2. Public Users.** Persons and organizations that are not University Users may only access University electronic communications resources or services under programs sponsored by the University, as authorized by the Chancellor, or for the Office of the President, the Senior Vice President, Business and Finance, for purposes of such public access in accordance with Section III.D, Allowable Use.
- 3. Transient Users.** Users whose electronic communications merely transit University facilities as a result of network routing protocols are not considered "Users" for the purposes of this Policy.

D. ALLOWABLE USES

Use of University electronic communications resources is allowable subject to the following conditions:

- 1. Purpose.** Electronic communications resources may be provided by University units or sub-units in support of the teaching, research, and public service mission of the University, and of the administrative functions that support this mission.
- 2. Non-Competition.** University electronic communications resources shall not be provided to individual consumers or organizations outside the University except by approval of the Chancellor. Such services shall support the mission of the University and not be in competition with commercial providers.
- 3. Restrictions.** University electronic communications resources may not be used for:

- unlawful activities;
 - commercial purposes not under the auspices of the University;
 - personal financial gain (except as permitted under applicable academic personnel policies);
 - personal use inconsistent with Section III.D, Allowable Uses; or
 - uses that violate other University or campus policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property and sexual or other forms of harassment (see Appendix B, References).
- 4. Representation.** Use of the University's name and seal is regulated by the State of California Education Code 92000. Users of electronic communications resources must abide by this statute as well as by University and campus policies on the use of the University's name, seals, and trademarks (see Appendix B, References). Users of electronic communications resources shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized to do so.
- 5. Endorsements.** Users of electronic communications resources must abide by University and campus policies regarding endorsements. References or pointers to any non-University entity contained in University electronic communications shall not imply University endorsement of the products or services of that entity.
- 6. False Identity and Anonymity.** Users of University electronic communications resources shall not, either directly or by implication, employ a *false identity* (the name or electronic identification of another). However, when not prohibited by law or other University policy, a supervisor may direct an employee to use the supervisor's identity to transact University business for which the supervisor is responsible. In such cases, an employee's use of the supervisor's electronic identity does not constitute a false identity.

A user of University electronic communications resources may use a *pseudonym* (an alternative name or electronic identification for oneself) for privacy or other reasons, so long as the pseudonym clearly does not constitute a false identity.

A user of University electronic communications resources may remain *anonymous* (the sender's name or electronic identification are hidden) except when publishing web pages and transmitting broadcasts.

Campus guidelines and procedures may further restrict the circumstances under which pseudonyms and anonymous electronic communications are permitted.

7. **Interference.** University electronic communications resources shall not be used for purposes that could reasonably be expected to cause excessive strain on any electronic communications resources, or to cause interference with others' use of electronic communications resources.

Users of electronic communications services shall not: (i) send or forward chain letters or their equivalents in other services; (ii) "spam," that is, exploit electronic communications systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited electronic messages; (iii) "letter-bomb," that is, send an extremely large message or send multiple electronic messages to one or more recipients and so interfere with the recipients' use of electronic communications systems and services; or (iv) intentionally engage in other practices such as "denial of service attacks" that impede the availability of electronic communications services.

8. **Personal Use.** University users of a University electronic communications facility or service may use that facility or service for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not: (i) interfere with the University's operation of electronic communications resources; (ii) interfere with the user's employment or other obligations to the University, or (iii) burden the University with noticeable incremental costs. When noticeable incremental costs for personal use are incurred, users shall follow campus guidelines and procedures for reimbursement to the University.

The California Public Records Act requires the University to disclose specified public records. In response to requests for such disclosure, it may be necessary to examine electronic communications records that users consider to be personal to determine whether they are public records that are subject to disclosure (see the presumption in Appendix A, Definitions, of a University Electronic Communications Record).

The University is not responsible for any loss or damage incurred by an individual as a result of personal use of University electronic communications resources.

9. **Accessibility.** All electronic communications intended to accomplish the academic and administrative tasks of the University shall be accessible to allowable users with disabilities in compliance with law and University policies. Alternate accommodations shall conform to law and University policies and guidelines.

10. Intellectual Property. The contents of all electronic communications shall conform to laws and University policies regarding protection of intellectual property, including laws and policies regarding copyright, patents, and trademarks. When the content and distribution of an electronic communication would exceed fair use as defined by the federal Copyright Act of 1976, users of University electronic communications resources shall secure appropriate permission to distribute protected material in any form, including text, photographic images, audio, video, graphic illustrations, and computer software.

E. ACCESS RESTRICTION

Eligibility to access or use University electronic communications services or electronic communications resources, when provided, is a privilege accorded at the discretion of the University. This privilege is subject to the normal conditions of use, including procedures for initiation and termination of service eligibility, established by the manager of the individual electronic communications resource.

In addition, use of University electronic communications resources may be restricted or rescinded by the University at its discretion when required by and consistent with law, when there is substantiated reason to believe that violations of law or University policies have taken place, when there are compelling circumstances, or under time-dependent, critical operational circumstances (see Appendix A, Definitions). Restriction of use is subject to established *campuswide* procedures or, in the absence of such procedures, to the approval of the appropriate Vice Chancellor(s) or, for the Office of the President, the Senior Vice President, Business and Finance. Electronic communications resource providers may, nonetheless, restrict use of University electronic communications systems and services on a temporary basis as needed in Emergency Circumstances and Compelling Circumstances (see Appendix A, Definitions).

In compliance with the Digital Millennium Copyright Act, the University reserves the right to suspend or terminate use of University electronic communications systems and services by any user who repeatedly violates copyright law.

IV. PRIVACY AND CONFIDENTIALITY

A. INTRODUCTION

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications. This Policy reflects these firmly-held principles within the context of the University's legal and other obligations. The University 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 the University's business.

The University does not examine or disclose electronic communications records without the holder's consent. Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the University may examine or disclose electronic communications under very limited circumstances as described in Section IV.B, Access Without Consent.

University employees are prohibited from seeking out, using, or disclosing personal information in electronic communications without authorization (see Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information). University policy requires that its employees take necessary precautions to protect the confidentiality of personal information encountered either in the performance of their duties or otherwise (see Business and Finance Bulletin IS-3, Electronic Information Security).

University contracts with outside vendors for electronic communications services shall explicitly reflect and be consistent with this Policy and other University policies related to privacy.

B. ACCESS WITHOUT CONSENT

An electronic communications holder's consent shall be obtained by the University prior to any access for the purpose of examination or disclosure of the contents of University electronic communications records in the holder's possession, except as provided for below.

The University shall permit the examination or disclosure of electronic communications records without the consent of the holder of such records only: (i) when required by and consistent with law; (ii) when there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of law or of University policies listed in Appendix C, Policies Relating to Access Without

Consent, have taken place; (iii) when there are compelling circumstances as defined in Appendix A, Definitions; or (iv) under time-dependent, critical operational circumstances as defined in Appendix A, Definitions.

When under the circumstances described above the contents of electronic communications records must be examined or disclosed without the holder's consent, the following shall apply:

- 1. Authorization.** Except in emergency circumstances (as defined in Appendix A, Definitions) in accordance with Section IV.B.2, Emergency Circumstances, or except for subpoenas or search warrants in accordance with Section IV.B.6, Search Warrants and Subpoenas, such actions must be authorized in advance and in writing by the responsible campus Vice Chancellor or, for the Office of the President, the Senior Vice President, Business and Finance (see Section II.D, Responsibilities).¹ This authority may not be further redelegated.

Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

- 2. Emergency Circumstances.** In emergency circumstances as defined in Appendix A, Definitions, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described in Section IV.B.1, Authorization, above.
- 3. Notification.** The responsible authority or designee shall at the earliest opportunity that is lawful and consistent with other University policy notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

Each campus will issue in a manner consistent with law an annual report summarizing instances of authorized or emergency nonconsensual access pursuant to the provisions of this Section IV.B, Access Without Consent, without revealing personally identifiable data.

- 4. Compliance with Law.** Actions taken under Sections IV.B.1, Authorization, and IV.B.2, Emergency Circumstances, shall be in full compliance with the law and other applicable University policies, including laws and policies listed in Appendix B, References. Advice of legal counsel must always be sought prior to any action involving electronic communications records (a)

¹ On March 18, 2004 the Regents Committee on Audit approved changes to the Internal Audit Management Charter authorizing Internal Audit to have access to University information except where prohibited by law. [<http://www.universityofcalifornia.edu/regents/regmeet/mar04.html>]

stored on equipment not owned or housed by the University, or (b) whose content is protected under the federal Family Educational Rights and Privacy Act of 1974 (see Section IV.C.1.b, Student Information).

5. **Recourse.** Campus implementing procedures shall specify the process for review and appeal of actions taken under Sections IV.B.1, Authorization, and IV.B.2, Emergency Circumstances to provide a mechanism for recourse to individuals who believe that actions taken by employees or agents of the University were in violation of this Policy.
6. **Search Warrants and Subpoenas.** Search warrants and subpoenas are not subject to sections 1-2 and 4-5 above. Search warrants and subpoenas for electronic communications records shall be referred to University legal counsel at the Office of the General Counsel or designated officials at campus locations.

Search Warrants. Duly signed search warrants shall be processed in accordance with federal and state laws, University policies, and instructions in the warrant.

Subpoenas. Subpoenas shall be processed in accordance with applicable federal and state laws and University policies (see Business and Finance Bulletin RMP-10, Instructions for Responding to Subpoena). Campus officials shall provide advance notice to individuals whose records are the subject of a subpoena duces tecum in accordance with instructions and time requirements in RMP-10, section III.C, “Responding to requests for personal records of a consumer.”

C. PRIVACY PROTECTIONS AND LIMITS

1. Privacy Protections

- a. **Personal Information.** Federal and California law provide privacy protections for some information that personally identifies an individual. Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information, provides guidelines for the collection and use of personal information in conformance with the law. These guidelines apply to information collected and disseminated by electronic means just as they do to records stored on paper and other media.
- b. **Student Information.** Users of electronic communications systems and services shall not disclose information about students in violation of the federal Family Educational Rights and Privacy Act of 1974 (FERPA), and the University policies that provide guidance in meeting FERPA requirements. See Business and Finance Bulletin RMP-8, Legal

Requirements on Privacy of and Access to Information, and 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).

- c. Electronically Gathered Data.** Any collection or distribution of personally identifiable information shall be consistent with federal and state law and University policy (see Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information). Except when otherwise provided by law, users of University electronic communications systems and services shall be informed whenever personally identifiable information other than transactional information (see Appendix A, Definitions) will be collected and stored automatically by the system or service.

In addition, California law requires state agencies and the California State University to enable users to terminate an electronic communications transaction without leaving personal data (see Appendix B, References). All electronic communications systems and services in which the University is a partner with a state agency or the California State University must conform to this requirement.

In no case shall electronic communications that contain personally identifiable information about individuals, including data collected by the use of "cookies" or otherwise automatically gathered, be sold or distributed to third parties without the explicit permission of the individual.

- d. Telephone Conversations.** In compliance with federal law, audio or video telephone conversations shall not be recorded or monitored without advising the participants unless a court has explicitly approved such monitoring or recording. Emergency services shall record 911-type emergency calls in accordance with federal and state laws and regulations.

Participants shall be informed when a call is being monitored or recorded for the purpose of evaluating customer service, assessing workload, or other business purpose permitted by law. University units that monitor or record telephone calls shall provide an alternative method of doing business with the University to clients who do not wish to be part of a monitored telephone call.

2. Privacy Limits

- a. **Possession of Public Records.** University employees shall comply with University requests for copies of public records in their possession, regardless of whether such records reside on University electronic communications resources.

- b. **System Monitoring.** University employees who operate and support electronic communications resources regularly monitor transmissions for the purpose of ensuring reliability and security of University electronic communications resources and services (see Section V.B, Security Practices), and in that process might observe certain transactional information or the contents of electronic communications. Except as provided elsewhere in this Policy or by law, they are not permitted to seek out transactional information or contents when not germane to system operations and support, or to disclose or otherwise use what they have observed.

In the process of such monitoring, any unavoidable examination of electronic communications (including transactional information) shall be limited to the least invasive degree of inspection required to perform such duties. This exception does not exempt systems personnel from the prohibition (see Section IV.A, Introduction) against disclosure of personal or confidential information..

Except as provided above, systems personnel shall not intentionally search the contents of electronic communications or transactional information for violations of law or policy. However, if in the course of their duties systems personnel inadvertently discover or suspect improper governmental activity (including violations of law or University policy), reporting of such violations shall be consistent with the Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (the "Whistleblower Policy").

- c. **Back-up Services.** Operators of University electronic communications resources shall provide information about back-up procedures to users of those services upon request.

V. SECURITY

A. INTRODUCTION

The University makes reasonable efforts to provide secure and reliable electronic communications services. Operators of University electronic communications resources are expected to follow appropriate professional practices in providing for the security of electronic communications records, data, application programs, and systems following guidelines provided in Business and Finance Bulletin IS-3, Electronic Information Security.

IS-3 provides guidelines for managing the security of electronic information resources used to conduct activities in support of the University's mission. IS-3 guidelines apply to the security of University electronic information resources in the form of electronic communications, stored data, and electronic communications resources used to transmit and process such records and data.

B. SECURITY PRACTICES

Providers of electronic communications services ensure the integrity and reliability of systems under their control through the use of various techniques that include routine monitoring of electronic communications. Network traffic may be inspected to confirm malicious or unauthorized activity that may harm the campus network or devices connected to the network. Such activity shall be limited to the least perusal of contents required to resolve the situation. User consent is not required for these routine monitoring practices. Providers shall document and make available to their users general information about these monitoring practices. If providers determine that it is necessary to examine suspect electronic communications records beyond routine practices, the user's consent shall be sought. If circumstances prevent prior consent, notification procedures described in Section IV.B.3, Notification shall be followed.

C. INTEGRITY

No person shall attempt to breach any security mechanisms that protect electronic communications services or facilities or any records or messages associated with these services or facilities unless otherwise authorized by other provisions of this Policy.

D. AUTHENTICATION

Electronic communications service providers (see Appendix A, Definitions) shall maintain currency with authentication technologies supported by the University and implement them in accordance with Business and Finance Bulletin IS-3, Electronic Information Security, and commensurate with applicable security requirements.

E. AUTHORIZATION

Service providers shall use authorization technologies commensurate with security requirements of the service, application, or system. See Business and Finance Bulletin IS-3, Electronic Information Security, for requirements regarding access management of the University's electronic information resources.

F. ENCRYPTION

Where deemed appropriate, electronic communications containing restricted data as defined in Business and Finance Bulletin IS-3, Electronic Information Security should be encrypted during transit across communications networks. Other communications may be encrypted during transit. All encrypted communications shall be handled upon receipt in conformance with the storage requirements for electronic information resources, as defined in IS-3.

G. RECOVERY

Providers of campuswide or Universitywide electronic communications services shall implement recovery practices adequate to ensure rapid recovery from security intrusions and service interruptions.

H. AUDIT

Providers of electronic communications services shall use cost-effective audit technologies and practices to help identify security violators and speed up recovery from security incidents. The use of such audit technologies and practices shall not conflict with other provisions of this Policy, in particular Section IV, Privacy and Confidentiality.

VI. RETENTION AND DISPOSITION

A. RETENTION

Electronic communications records are subject to University records management policies as stated in the University of California Records Disposition Schedules Manual, which provides guidance for administering the retention and disposition of all records, regardless of the medium on which they are stored.

B. DISPOSITION

The Record Proprietor, as defined in Business and Finance Bulletin RMP-1, University Records Management Program, is responsible for preserving those electronic communications records that have been identified as having lasting business purpose or historical value to the University.

C. BACK-UP

The University does not maintain central or distributed electronic archives of all electronic communications records sent or received. Electronic communications records are normally backed up, if at all, only to assure system integrity and reliability, not to provide for future retrieval, although back-ups may at times serve the latter purpose incidentally. Operators of University electronic communications services are not required by this Policy to routinely retrieve electronic communications records from such back-up facilities for individuals.

APPENDIX A: DEFINITIONS

Compelling Circumstances: Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policies listed in Appendix C, Policies Relating to Access Without Consent, or significant liability to the University or to members of the University community.

Electronic Communications: Any transfer of signals, writings, images, sounds, data or intelligence that is, created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems². For purposes of this Policy, an electronic file that has not been transmitted is not an electronic communication.

Electronic Communications Records: The contents of electronic communications created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems or services. This definition of electronic communications records applies equally to attachments to such records and transactional information associated with such records.

Electronic Communications Resources: Telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications services.

Electronic Communications Service Provider: Any unit, organization, or staff with responsibility for managing the operation of and controlling individual user access to any part of the University's electronic communications systems and services.

Electronic Communications Systems or Services: Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

² Definition is modeled on language contained in the Electronic Communications Privacy Act (see US Code Title 18 § 2510).

Emergency Circumstances: Circumstances in which time is of the essence and there is a high probability that delaying action would almost certainly result in compelling circumstances.

Faculty: A member of the faculty as defined by Academic Personnel Policy 110-4 (14).

Holder of an Electronic Communications Record or Electronic Communications

Holder: An electronic communications user who, at a given point in time, is in possession (see definition below) or receipt of a particular electronic communications record, whether or not that electronic communications user is the original creator or a recipient of the content of the record.

Possession of Electronic Communications Record: An individual is in possession of an electronic communications record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage or access to its content. Thus, an electronic communications record that resides on an electronic communications server awaiting download to an addressee is deemed, for purposes of this Policy, to be in the possession of that addressee. Systems administrators and other operators of University electronic communications services are excluded from this definition of possession with regard to electronic communications not specifically created by or addressed to them.

- Electronic communications users are not responsible for electronic communications records in their possession when they have no knowledge of the existence or contents of such records.

Public Record: A record as defined in Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information, and/or the California Public Records Act. Public records include writings or other forms of recording that contain information relating to the conduct of the public's business in materials prepared, owned, used, or retained by the University regardless of physical form or characteristics [California Government Code Section 6252(e)]. Except for certain defined situations, such records are subject to disclosure under the California Public Records Act. For more information regarding the requirements of the Public Records Act, and the University's implementation of that Act, including exemptions from disclosure, see RMP-8.

Substantiated Reason: Reliable evidence indicating that violation of law or of University policies listed in Appendix C, Policies Relating to Access Without Consent, probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

Time-dependent, Critical Operational Circumstances: Circumstances in which failure to act could seriously hamper the ability of the University to function administratively or to meet its teaching obligations, but excluding circumstances pertaining to personal or professional activities, or to faculty research or matters of shared governance.

Transactional Information: Information, including electronically gathered information, needed either to complete or to identify an electronic communication. Examples include but are not limited to: electronic mail headers, summaries, addresses and addressees; records of telephone calls; and IP address logs.

University Administrative Record: A Public Record (see definition above) that documents or contains information related to the organization, functions, policies, decisions, procedures, operations, or other business activities of the University.

University Electronic Communications Record: A Public Record in the form of an electronic communications record, whether or not any of the electronic communications resources utilized to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print the electronic communications record are owned by the University. This implies that the location of the record, or the location of its creation or use, does not change its nature (i) as a University electronic communications record for purposes of this or other University policy, and (ii) as having potential for disclosure under the California Public Records Act.

- Until determined otherwise or unless it is clear from the context, any electronic communications record residing on university-owned or controlled telecommunications, video, audio, and computing facilities will be deemed to be a University electronic communications record for purposes of this Policy. This *would* include personal electronic communications. Consistent with the principles of least perusal and least action necessary and of legal compliance, the University must make a good faith a priori effort to distinguish University electronic communications records from personal and other electronic communications in situations relevant to disclosures under the California Public Records Act and other laws, or for other applicable provisions of this Policy.

University Electronic Communications Systems or Services: Electronic communications systems or services owned or operated by the University or any of its sub-units or provided through contracts with the University.

Use of Electronic Communications Services: To create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print electronic communications with the aid of electronic communications services. An Electronic Communications User is an individual who makes use of electronic communications services.

- The act of receipt of electronic communications as contrasted with actual viewing of the record by the recipient is excluded from the definition of "use" to the extent that the recipient does not have advance knowledge of the contents of the electronic communications record.

APPENDIX B: REFERENCES

The following list identifies significant sources used as background in the preparation of this Policy, whether or not they are directly referenced by this Policy. It does not include all applicable laws and University policies. Laws and policies change from time to time, so users of this Policy are encouraged to refer to the Office of the President Universitywide Policy Manuals and Selected Guidelines website at <http://www.ucop.edu/ucophome/coordrev/ucpolicies/policymanuals.html> for updates.

University Policies and Guidelines

- ***Business and Finance Bulletins:***

- A-56, Academic Support Unit Costing and Billing Guidelines
- BUS-29, Management and Control of University Equipment
- BUS-43, Materiel Management
- BUS-65, Guidelines for University Mail Services
- IS-3, Electronic Information Security
- RMP-1, University Records Management Program
- RMP-2, Records Retention and Disposition
- RMP-7, Privacy of and Access to Information Responsibilities
- RMP-8, Legal Requirements on Privacy of and Access to Information
- RMP-10, Instructions for Responding to Subpoena

- ***Personnel Manuals and Agreements:***

- Academic Personnel Manual
- Personnel Policies for Staff Members and Appendix II for Senior Managers
- Collective Bargaining Contracts (Memoranda of Understanding)

- ***Other Related Policies and Guidelines:***

- Campus Access Guidelines for Employee Organizations (Local Time, Place, and Manner Rules)
- Policies Applying to Campus Activities, Organizations, and Students
- Policy and Guidelines on the Reproduction of Copyrighted Materials for Teaching and Research
- Policy on Copyright Ownership (1992) and the 2003 Policy on Ownership of Course Materials
- Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (the "Whistleblower Policy")

Policy on Sexual Harassment and Procedures for Responding to Reports of Sexual Harassment
University of California Records Disposition Schedules Manual
University Policy on Integrity in Research

State of California Statutes

State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)
State of California Public Records Act (Government Code Section 6250 et seq.)
State of California Education Code, Section 67100 et seq.
State of California Education Code 92000
State of California Government Code, Section 11015.5
State of California Penal Code, Section 502 and 1523 et seq.

Federal Statutes and Regulations

Americans with Disabilities Act of 1990
Communications Decency Act of 1996
Copyright Act of 1976
Digital Millennium Copyright Act of 1998
Electronic Communications Privacy Act of 1986
Family Educational Rights and Privacy Act of 1974
Health Insurance Portability and Accountability Act of 1996
Privacy Act of 1974
Telecommunications Act of 1934
Telecommunications Act of 1996
Federal Communications Commission Rules and Regulations

APPENDIX C: POLICIES RELATING TO ACCESS WITHOUT CONSENT

The Electronic Communications Policy cites circumstances under which access to electronic communications may occur without the prior consent of the holder (see Section IV.B, Access Without Consent). Following are University policies that may trigger nonconsensual access following procedures defined in Section IV.B, Access Without Consent.

1. University policies governing sexual or other forms of harassment, specifically: Policies Applying to Campus Activities, Organizations, and Students, Section 160; Section APM-035, Appendix A of Affirmative Action and Nondiscrimination in Employment; and Personnel Policies for UC Staff Members. Sexual harassment concerning students is covered by item 6 below.
2. Certain portions of policies governing access to University records, specifically RMP-1, Section IV.B; RMP-8, Sections on Disclosure of Information and Rules of Conduct.
3. The Academic Personnel Manual, APM-015, Section II, Part II, Professional Responsibilities, Ethical Principles, and Unacceptable Faculty Conduct, and the University Policy on Integrity in Research, APM 190, Appendix B.
4. Personnel Policies for Staff Members and Appendix II for Senior Managers
5. Collective bargaining agreements and memoranda of understanding.
6. Section 102 governing student conduct of the policy entitled Policies Applying to Campus Activities, Organizations, and Students.
7. Sections III, Allowable Use, and IV, Privacy and Confidentiality, of this Electronic Communications Policy.

Violations of other policies can normally be detected and investigated without requiring nonconsensual access to electronic communications. On occasion, attention to possible policy violations is brought about because of the receipt by others of electronic communications. However, it is acknowledged that electronic communications can be forged, the true identity of the sender can be masked, and the apparent sender might deny authorship of the electronic communication. In such circumstances and provided there is substantiated reason (as defined in Appendix A, Definitions) that points to the identity of the sender, nonconsensual access to the purported sender's electronic communications may be authorized following the procedures defined in Section IV.B, Access Without

Consent, but only to the least extent necessary for verifying unambiguously the identity of the sender, and only for major violations of the following policies:

- Business and Finance Bulletin A-56, Section IV.H, governing sales of goods or services outside the University.
- Business and Finance Bulletin BUS-29, Section N, governing use of University materiel or property.
- Business and Finance Bulletin BUS-43, Part 3, Section X.A, governing use of University credit, purchasing power, or facilities.
- Policies Applying to Campus Activities, Organizations, and Students, Section 42.40, governing use of University properties for commercial purposes and personal financial gain.
- Business and Finance Bulletin BUS-65, Section VII, governing provision of University mailing lists to others.
- Policy and Guidelines on the Reproduction of Copyrighted Materials for Teaching and Research.
- Campus Access Guidelines for Employee Organizations.

Posting and Authority to Change

Because University policies are subject to change, this list may change from time to time. The authoritative list at any time will be posted under the listings of University policies posted on the Web. Authority to change this list rests with the President of the University acting, where policies affecting faculty are concerned, with the advice of the Academic Senate.

ECP SUPPORTING DOCUMENTS

[Attachment 1 User Advisories](#)

[Attachment 2 Implementation Guidelines](#)

Electronic Communications Policy

Attachment 1

User Advisories

University of California
Office of the President

Issued November 17, 2000

Revised August 18, 2005

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	USER RESPONSIBILITIES	1
A.	COMPLIANCE WITH LAW.....	1
B.	ALLOWABLE USES	1
C.	COURTESY.....	2
III.	PRIVACY EXPECTATIONS	2
IV.	PRIVACY PROTECTIONS	3
A.	PERSONAL INFORMATION	3
B.	STUDENT PRIVACY	3
C.	ELECTRONIC DATA GATHERING	4
V.	PRIVACY LIMITS.....	4
A.	INTRODUCTION.....	4
B.	PUBLIC RECORDS	4
C.	UNIVERSITY POLICIES	5
D.	UNINTENDED DISTRIBUTION	5
E.	ELECTRONIC DATA GATHERING	6
VI.	SECURITY CONSIDERATIONS.....	6
A.	SECURITY	6
B.	AUTHENTICATION	7
C.	BACK-UP.....	7
D.	DISPOSITION	7

I. INTRODUCTION

University policies often interpret the application of federal and state laws to the University community. The Electronic Communications Policy interprets the application of other University policies, as well as federal and state laws, to electronic communications. Users of electronic communications who are in doubt concerning the permissibility of an intended action should seek guidance from the Universitywide Electronic Communications Policy and, where they exist, local campus implementing guidelines and other computer policies that may interpret policy or address areas not explicitly covered by Universitywide policies.

II. USER RESPONSIBILITIES

A. COMPLIANCE WITH LAW

The Electronic Communications Policy refers to federal laws that prohibit:

- Monitoring telephone conversations without informing participants or without a court order;
- Using the Internet to make available intellectual property belonging to another in such a way as to cause the loss of \$2500 or more;
- Infringing copyright by electronic communications.

The Electronic Communications Policy refers to California laws that govern the use of computer equipment, systems and services, and which apply to electronic communications as well. Section 502 of the California Penal Code prescribes criminal penalties for:

- Using electronic means to defraud others;
- Using data or documentation without permission;
- Using electronic equipment without permission;
- Tampering with data, software, or programs;
- Disrupting or causing denial of services to authorized users;
- Accessing or providing access to others without permission;
- Introducing computer contaminants, such as viruses; and
- Using the Internet domain name of another.

In general, behaviors that are prohibited in the physical environment are also prohibited in the digital environment.

B. ALLOWABLE USES

The Electronic Communications Policy identifies ten principles that govern the allowable use of University electronic communications resources. Users are advised

to review local campus computing guidelines that specify how these are implemented and enforced at each University location (see Electronic Communications Policy, Section III.D, Allowable Use).

In accordance with federal law, users should assume that material created by others, in electronic or other form, is protected by copyright unless such material includes an explicit statement that it is not protected, or unless such material is clearly in the public domain (see the Electronic Communications Policy, Section III.D.10, Intellectual Property).

C. COURTESY

The University cannot protect users of University electronic communications resources from receiving communications they may not wish to receive. Members of the University community are strongly encouraged to use the same personal and professional courtesies and considerations in electronic communications as they would in other forms of communication (see Electronic Communications Policy, Section IV.A, Introduction).

III. PRIVACY EXPECTATIONS

Various laws and available security technologies affect the degree of privacy that users can expect. Generally, laws relating to more mature communications technologies are more fully developed than those governing newer technologies as a result of court interpretations that have led to consensus about their application. For example, laws that circumscribe the privacy of telephone communications are well established while those that apply to electronic mail are not. While some laws support higher expectations of privacy, other laws interfere with such expectations (see Electronic Communications Policy, Section IV.C, Privacy Protections and Limits).

Users commonly associate different levels of privacy with various electronic communications technologies or with alternative uses of those technologies. For example:

- Users generally expect a high level of privacy with telephone conversations, and these expectations are generally protected by law;
- Users often expect a similarly high level of privacy with electronic mail, but (i) these expectations are not always supported by law, and (ii) recipients may compromise confidentiality by redirecting electronic mail messages;
- Users might expect a more moderate level of privacy with electronic communications intended for distribution to a limited audience, since privacy can be compromised by the limit of available security protections or by the behavior

of members of the intended audience (a user, for example, might share a password without knowledge or consent of the originator of the communication); and

- Users should expect minimal or no privacy in broadcast communications, such as television or unprotected web pages, because they are accessible to a wide, unspecified audience.

IV. PRIVACY PROTECTIONS

Two categories of information that are protected from disclosure by law are information that personally identifies an individual and certain information pertaining to students. In addition, state and federal laws partially limit the use of automated electronic data gathering tools to collect and store personally identifiable information about individuals without their knowledge or consent (see Electronic Communications Policy, Section IV, Privacy and Confidentiality). In spite of these legal protections users of electronic communications should exercise caution to protect their privacy.

A. PERSONAL INFORMATION

Users of electronic communications systems and services should be aware of the difficulty of maintaining privacy and confidentiality on the web and should be particularly careful about posting personal information on the web. They should note that even web pages that have no pointers to or from other web pages might be found by search engines.

Users who do not want their electronic mail addresses made public are cautioned not to send electronic communications to mailing list systems, chat rooms, web pages, and newsgroups where they might be discovered or otherwise used for purposes over which the individual has no control.

B. STUDENT PRIVACY

Federal law protecting student privacy is incorporated into University policies. 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), campuses are responsible for designating the categories of personally identifiable information about a student that are public. Individual students may, consistent with the above policy, request the campus not to make public their electronic mail addresses and telephone numbers (see Electronic Communications Policy, Section II.D, Responsibilities and Section IV.C, Privacy Protections and Limits).

C. ELECTRONIC DATA GATHERING

Legislation protecting the privacy of electronic communications users is still evolving. There are currently few laws that would adequately protect users from electronic data gathering without their permission (see Electronic Communications Policy Section V.C, Privacy Protections and Limits).

V. PRIVACY LIMITS

A. INTRODUCTION

The privacy of electronic communications at the University is limited by: i) laws that protect the public's right to know about the public business; ii) policies that require employees to comply with management requests for University records in their possession; and iii) technical requirements for efficient operation of University electronic communications resources (see Electronic Communications Policy, Section IV, Privacy & Confidentiality). Privacy and confidentiality might also be compromised by unintended redistribution or by the inadequacy of current technologies to protect against unauthorized access. Therefore, users should exercise extreme caution in using electronic communications to transmit confidential or sensitive matters. Guidance on storage, disposal, and preservation of records is addressed in the Appendices to RMP-2, "Records Retention and Disposition: Principles, Processes, and Guidelines."

B. PUBLIC RECORDS

Users of University electronic communications services should be aware that the California Public Records Act and other similar laws make it impossible for the University to guarantee complete protection of an individual's personal electronic communications records resident on University facilities (see Electronic Communications Policy Section III.D.8, Personal Use).

The University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the California Public Records Act, other laws concerning disclosure and privacy, and other applicable law. Business and Finance Bulletin RMP-8 and personnel manuals and agreements provide guidelines for University implementation of the California Public Records Act.

Electronic communications records arising from personal use may be difficult to distinguish from public records, and such records may be subject to inspection or disclosure pursuant to the California Public Records Act (see the presumption in the

Electronic Communications Policy, Appendix A, Definitions, of a University Electronic Communications Record, regarding personal and other electronic communications records). Users should assess the implications of this presumption in their decision to use University electronic communications resources for personal purposes.

The California Public Records Act does not in general apply to records generated or held by students except in their capacity, if any, as employees or agents of the University. This exemption only applies to the Act and does not exclude students' electronic communications from other aspects of this Policy.

C. UNIVERSITY POLICIES

In addition to University policies that require employees to comply with management requests for University records in their possession, other University policies affect the privacy of some forms of electronic communication.

In compliance with law, the University does not record or monitor audio or video telephone conversations except as described below, unless under court order. The law permits the University to monitor or record calls for the purpose of evaluating customer service, assessing workload, or other business purposes. In such cases the University advises the participants that the call is being monitored or recorded. Users who do not wish to be part of a monitored telephone call should be aware that University units are required to provide them with an alternative method of doing business with the University (see Electronic Communications Policy, Section IV.C. Privacy Protections and Limits).

The use of University telephone equipment creates transaction records (which include the number called and the time and length of the call) that are reviewed by University units and sub-units as part of routine accounting procedures. Employees who use University telephones for personal or other purposes should be aware that supervisors have access to records of all calls made from University telephones under their jurisdiction and that such records may be used for administrative purposes.

D. UNINTENDED DISTRIBUTION

Both the nature of electronic mail and the public character of the University's business make electronic mail less private than users might anticipate. For example, electronic mail intended for one person sometimes might be widely distributed because of the ease with which recipients can forward it to others. A reply to an electronic mail message posted on an electronic bulletin board or mailing list system intended only for the originator of the message might be distributed to all subscribers to the mailing list system. Users of workstations in public computer laboratories might forget to remove files after they finish their work. Even after a user deletes an

electronic mail record, it might persist on back-up or local facilities and become subject to disclosure under the provisions of Section IV.B, Access Without Consent, of this Policy. The University cannot routinely protect users against such eventualities.

Users of telephone, video teleconference, and other telecommunications services are advised that although electronic communications are subject to the non-consensual access provisions of the Electronic Communications Policy Section IV.B, their privacy might be compromised by the presence of persons listening to speaker phones or participating in teleconference calls and video teleconferences without announcing their presence.

E. ELECTRONIC DATA GATHERING

Users of electronic communications systems or services should also be aware that by accessing electronic communications resources, users create transaction records that leave a trail of the electronic communications resources used and might give information about the users and their activities. Current state and federal laws governing such electronic data gathering may not fully protect the user from the gathering of such information without their knowledge or consent. Users are advised to read the privacy statement of any application that collects personally identifiable information to learn its disclosure and privacy policies.

VI. SECURITY CONSIDERATIONS

A. SECURITY

Encryption technology enables the encoding of electronic communications so that for all practical purposes they cannot be read by anyone who does not possess the commensurate technology needed to decrypt them. Users of electronic communications services should be aware that the University does not routinely encrypt electronic communications during transit across its facilities. If there is a concern about possible interception or disclosure of electronic communications, correspondents should implement appropriate encryption technology while ensuring conformance with BFB IS-3.

Since the University is not responsible for any loss or damage incurred by an individual as a result of personal use of University electronic communications resources, users should not rely on personal use of University electronic communications resources for communications that might be sensitive with regard to timing, financial effect, or privacy and confidentiality. (See the Electronic Communications Policy, Section III.D.8, Personal Use.)

B. AUTHENTICATION

Unless authentication technologies are in use, there is no guarantee that an electronic communication received was in fact sent by the purported sender, since it is relatively straightforward, although a violation of the Electronic Communications Policy, for senders to falsify their identity. Electronic communications that are forwarded might also be modified. General purpose (in contrast to application specific) authentication technologies are not widely and systematically in use at the University as of the issuance of the Policy, but can be expected in future.

As with print documents, recipients of electronic communications should, in case of doubt, check directly with the purported sender to validate the authenticity of the sender or the content.

C. BACK-UP

Electronic communications systems are backed up on a routine or occasional basis to protect system reliability and integrity, and to prevent potential loss of data. The back-up process entails the copying of electronic data onto storage media that might be retained for periods of time and in locations unknown to the originator or recipient of electronic communications. The practice and frequency of back-ups and the retention of back-up copies vary from system to system. Users are encouraged to request information on local back-up practices followed by the operators of University electronic communications resources, and such operators are required to provide such information to users upon request (see the Electronic Communications Policy, Section IV.C, Privacy Protections and Limits).

Users of electronic communications resources should be aware that even if they have discarded copies of an electronic communication stored on devices they can control, back-up copies could exist on other devices. Back-up copies that are able to be retrieved might be subject to disclosure under the California Public Records Act or, in litigation, as the result of the discovery process.

D. DISPOSITION

Electronic communications users should be aware that generally it is not possible to assure the longevity of electronic communications records for record-keeping purposes, in part because of the difficulty of guaranteeing that they can continue to be read in the face of changing formats and technologies, and in part because of the changing nature of electronic communications systems. Archiving is increasingly difficult as electronic communications encompass more digital forms, such as compound records composed of digital voice, music, image, and video in addition to text. In the absence of the use of authentication systems it is difficult to guarantee that electronic communications have not been intentionally or inadvertently altered (see

the Electronic Communications Policy, Section IV.C, Privacy Protections and Limits and Section V.C, Authentication).

Those in possession of University records in the form of electronic communications are cautioned, therefore, to be prudent in their reliance on electronic means for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to the feasibility of transferring electronic communications records to a more lasting medium or format, such as acid-free paper or microfilm, for long-term accessibility as required.

Electronic Communications Policy

Attachment 2 Implementation Guidelines

University of California
Office of the President

Issued November 17, 2000
Revised August 18, 2005
Revised April 7, 2011

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PURPOSE	1
B.	CAMPUS RESPONSIBILITIES	1
II.	ALLOWABLE USE.....	3
A.	ALLOWABLE USERS.....	3
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 in accordance with these Implementation Guidelines in consultation with campus faculty, students, and staff.

1. Each Chancellor shall designate a coordinator to administer the Policy and campus implementing guidelines.
2. 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.
3. 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.
4. 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.
5. 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.

6. 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).
7. 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.
8. 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).
9. Each Chancellor may establish additional procedures that further refine and conform with this Policy.
10. 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 communications 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 communications 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 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 include the following requirements:
 - 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.
 - Advice of campus legal 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 search warrant, subpoena, or subpoena duces tecum, in accordance with Policy Section IV.B, Access without Consent, 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 examination or disclosure involves electronic communications held by faculty.
3. **Notification.** Advice of legal 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. **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. Access that results from search

warrants, subpoenas, subpoenas duces tecum or other court orders shall be included in annual reports.

- 5. 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. System Monitoring.** 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.b, System Monitoring, 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. Providers of electronic communications services shall document and make available general information about the monitoring practices of systems under their control consistent with Policy Section V.B. Security Practices. This information shall include types of monitoring activities, the level of inspection required to examine suspect electronic communications records, and accompanying procedures. This information serves to meet the ECP provision requiring the documentation of routine monitoring practices.

For purposes of the Electronic Communications Policy, automated inspection of electronic communications in order to protect the integrity and reliability of University electronic communications resources does not constitute

nonconsensual access (see Electronic Communications Policy Sections III.D.7, Interference, IV.C.2.b, System Monitoring, 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 electronic communications records in the event of absence, campuses are encouraged to use techniques or procedures to minimize the need to gain access without consent. Following are some practices that campuses may implement.

- *"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).
- *Workgroup accounts.* Establish common workgroup accounts for department-related business so essential departmental business electronic communications are accessible to all workgroup members.
- *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 file server capability to store and access documents in support of business operations. Authorization and access procedures must be clearly documented.

Campuses may also establish a central campus approval process to obtain pre-approved user consent to allow access to user's electronic communications records. Each agreement must be on a case-by-case basis rather than for groups, and the agreement must address only narrowly defined circumstances, e.g., emergency medical leave, when such access is to be obtained.

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 separation.
- 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 separation 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 communications 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.

6. Monitoring of Access to Patient and Student Information Records.

Patient and student information records are collected, stored, and accessed for business purposes only. Routine monitoring of access to institutional databases or other institutional collections of patient and student information records is a recommended information security practice and is not subject to the nonconsensual access provisions of the Electronic Communications Policy, Section IV.B.

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.