

Electronic Communications Policy

University of California
Office of the President

November 17, 2000

TABLE OF CONTENTS

| | | |
|-------------|--|-----------|
| I. | INTRODUCTION..... | 1 |
| II. | GENERAL PROVISIONS | 2 |
| | A. PURPOSE | 2 |
| | B. SCOPE | 2 |
| | C. DEFINITIONS | 3 |
| | D. RESPONSIBILITIES..... | 4 |
| | 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 MECHANISMS..... | 15 |
| | C. AUTHENTICATION | 15 |
| | D. AUTHORIZATION | 15 |
| | E. ENCRYPTION | 16 |
| | F. RECOVERY | 16 |
| | G. AUDIT | 16 |
| VI. | RETENTION AND ARCHIVING..... | 17 |
| | A. RETENTION | 17 |
| | B. ARCHIVING | 17 |
| | C. BACK-UP | 17 |
| | APPENDIX A: DEFINITIONS | 18 |
| | APPENDIX B: REFERENCES..... | 22 |
| | APPENDIX C: POLICIES RELATING TO ACCESS WITHOUT CONSENT | 24 |

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, this Policy establishes an overall policy framework for electronic communications. This Policy establishes new policy and procedures where existing policies do not specifically address issues particular to the use of electronic communications. It also clarifies the applicability of law and of other University policies to electronic communications. Where possible, this Policy defers to other University policies.

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 herein) 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 records and 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 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
- Substantiated Reason
- Time-dependent, Critical Operational Circumstances
- Transactional Information
- University Administrative Record
- University Electronic Communications Record
- University Electronic Communications Systems or Services
- University Record
- 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, or for the Office of the President, the Senior Vice President, Business and Finance, shall develop, maintain, and publish specific procedures and practices that implement this Policy, including information on accessibility of student information, authorized users, procedures for restricting or denying access, adjudication of complaints, and other matters as described in Attachment 2, Implementation Guidelines.
3. **Informational Material.** Campuses shall provide users of University electronic communications resources with understandable instructional material based on this Policy and on their own campus implementation guidelines.

E. VIOLATIONS OF LAW AND POLICY

1. **Sanctions of Law.** Both 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 any possible legal sanctions, violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion, as relevant, 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 access to its electronic communications resources 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 communications 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, 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 (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 University 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, not owned by The Regents, may also be subject to disclosure as University 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 or sub-unit of the University or assigned by the University to individuals, units, sub-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 or any of its sub-units, 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 or sub-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 within 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, 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 directly or indirectly cause excessive strain on any electronic communications resources, or unwarranted or unsolicited interference with others' use of electronic communications resources.

Users of electronic communications services shall not: (i) send or forward electronic mail 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 communications; (iii) "letter-bomb," that is, send an extremely large message or send multiple electronic communications to one or more recipients to 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) directly or indirectly 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 access 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

Access to and use of 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 access, established by the manager of the individual electronic communications resource.

In addition, access to and use of University electronic communications services or electronic communications resources may be wholly or partially restricted or rescinded by the University without prior notice and without the consent of the electronic communications user 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 access and use under such conditions is subject to established *campuswide* procedures or, in the absence of such procedures, to the approval of the appropriate campus Vice Chancellor(s) or, for the Office of the President, the Senior Vice President, Business and Finance. Electronic communications resource providers may, nonetheless, restrict access to University electronic communications systems and services on a temporary basis as needed in Emergency Circumstances and Compelling Circumstances (see Appendix A, Definitions) in order to control an emergency or prevent damage or loss.

In compliance with the Digital Millennium Copyright Act, the University reserves the right to suspend or terminate access to 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 routinely inspect, monitor, or disclose electronic communications without the holder's (as defined in Appendix A, Definitions) consent. Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the University may deny access to its electronic communications services and may inspect, monitor, or disclose electronic communications under very limited circumstances as described in Sections III.E, Access Restriction, and IV.B, Access Without Consent.

University policy (see Business and Finance Bulletin RMP-8) prohibits University employees and others from "seeking out, using, or disclosing" personal information without authorization, and requires employees to take necessary precautions to protect the confidentiality of personal information encountered in the performance of their duties or otherwise. This prohibition applies to electronic communications. In this Policy the terms "inspect, monitor, or disclose" are used within the meaning of "seek, use, or disclose" as defined in RMP-8.

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

The University shall only permit the inspection, monitoring, or disclosure of electronic communications records without the consent of the holder of such

records: (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 Non-Consensual Access, 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 must be inspected, monitored, or disclosed without the holder's consent, the following shall apply:

- 1. Authorization.** Except in emergency circumstances as defined in Appendix A, Definitions, and pursuant to Section IV.B.2, Emergency Circumstances, 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). 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.** In either case, the responsible authority or designee shall at the earliest possible 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 non-consensual 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 Counsel must always be sought prior to any action involving electronic communications (a) 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.

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.

C. PRIVACY PROTECTIONS AND LIMITS

1. Privacy Protections

- a. **Personal Information.** Both 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 RMP-8 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.** 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. Any other distribution of such information shall be consistent with University policy (see Business and Finance Bulletin RMP-8).

- 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 and sub-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. Public Records.** Records of electronic communications pertaining to the business of the University, whether or not created or recorded on University equipment, are University records (see Appendix A, Definitions) subject to disclosure under the California Public Records Act, other laws, or as a result of litigation.
- b. Possession of University Records.** University employees are expected to comply with University requests for copies of records in their possession that pertain to the business of the University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on University electronic communications resources.
- c. Unavoidable Inspection.** During the performance of their duties, personnel who operate and support electronic communications resources periodically need to monitor transmissions or observe certain transactional information to ensure the proper functioning and security of University electronic communications resources and services. On these and other occasions, systems personnel might observe the contents of electronic communications. Except as provided elsewhere in this Policy or by law, they are not permitted to seek out the contents or transactional information

where not germane to the foregoing purposes, or disclose or otherwise use what they have observed.

Such unavoidable inspection of electronic communications is 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 and confidential information, except insofar as such disclosure equates with good faith attempts to route an otherwise undeliverable electronic communication to its intended recipients.

Except as provided above, systems personnel shall not intentionally search electronic communications records or transactional information for violations of law or policy. However, as required by Business and Finance Bulletin G-29, Procedures for Investigating Misuse of University Resources, they shall report violations discovered inadvertently in the course of their duties.

- d. **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 attempts to provide secure and reliable electronic communications services. Operators of University electronic communications resources are expected to follow sound professional practices in providing for the security of electronic communications records, data, application programs, and systems under their jurisdiction based on the guidelines provided in Business and Finance Bulletin IS-3, Electronic Information Security.

Business and Finance Bulletin IS-3, Electronic Information Security, provides guidelines for managing the security of electronic information resources used in support of the University's administrative functions. IS-3 guidelines apply to University administrative records in the form of electronic communications, stored administrative data, and electronic communications resources used to transmit and access such records and data.

B. SECURITY MECHANISMS

Unless otherwise authorized by other provisions of this Policy, no person shall breach or attempt to breach any security mechanisms used by the University to protect electronic communications services or facilities, or any records or messages associated with these services or facilities.

C. AUTHENTICATION

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

D. AUTHORIZATION

Service providers shall implement and employ authorization technologies commensurate with the security requirements of the service, application, or system. Business and Finance Bulletin IS-3, Electronic Information Security, defines specific requirements regarding the University's administrative electronic resources.

E. ENCRYPTION

Transit. Electronic communications records may be *encrypted* during transit across communications networks.

Storage. Records subject to disclosure under the California Public Records Act (see Business and Finance Bulletin RMP-8) or required to be accessible for defined periods of time in compliance with the University of California Records Disposition Schedules Manual shall be stored in an *unencrypted* format.

F. RECOVERY

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

G. AUDIT

Providers of electronic communications services shall implement and employ cost-effective audit technologies and practices to help identify security violators and speed up recovery from security violations. 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 ARCHIVING

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 to University units and sub-units in administering the retention or disposition of all records, regardless of the medium on which they are stored.

B. ARCHIVING

Electronic communications records that have been identified as having lasting or historical value to the University shall be properly preserved in the Office of Record as identified in University of California Records Disposition Schedules Manual.

C. BACK-UP

The University does not maintain central or distributed electronic archives of all electronic communications sent or received. Electronic communications 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 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 Non-Consensual Access, or significant liability to the University or to members of the University community.

Electronic Communications: Any communication that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems or services. For purposes of this Policy, an electronic file that has not been transmitted is not an electronic communication.

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

Electronic Communications Resources: Any combination of 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, 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.

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.

Substantiated Reason: Reliable evidence indicating that violation of law or of University policies listed in Appendix C, Policies Relating to Non-Consensual Access, 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 University Record (see definition below) that is directly related to the conduct of the University's administrative business.

University Electronic Communications Record: A University 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, 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.

University Record: A "public record" as defined in Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information, and the California Public Records Act. Public records include writing 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(d)]. Except for certain defined situations, such University records are subject to disclosure under the California Public Records Act.

- In general, records held by students, including electronic communications records, are not University records unless such records exist pursuant to an employment or agent relationship the student has or has had with the University. This exemption applies only to the California Public Records Act; student electronic communications records are subject to all other provisions of this Policy, whether or not the electronic communications record is a University record.

Use of Electronic Communications Services: To create, send, forward, reply to, transmit, 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 federal and state laws and University policies that may have application to electronic communications. Since laws and University policies change from time to time, users of this Policy are encouraged to refer to the Office of the President World Wide Web site 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
- G-29, Procedures for Investigating Misuse of University Resources
- IS-3, Electronic Information Security
- RMP-1, University Records Management Program
- RMP-2, Records Disposition Program and Procedures
- RMP-7, Privacy of and Access to Information Responsibilities
- RMP-8, Legal Requirements on Privacy of and Access to Information

- ***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
- Policy on Sexual Harassment and Complaint Resolution Procedures
- 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

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
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 non-consensual 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 the Faculty Code of Conduct; 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 III; RMP-8, Section VII.G; and RMP-8, Exhibit D.
3. The Academic Personnel Manual, APM-015, Section II, Part II, limited to those parts headed Unacceptable Faculty Conduct, and the University Policy on Integrity in Research.
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 non-consensual 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, non-consensual access to the purported sender's electronic communication 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 might change from time to time. The authoritative list at any time will be posted under the listings of University policies posted on the World Wide 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.