

UNIVERSITY OF CALIFORNIA
OFFICE OF THE PRESIDENT
ELECTRONIC MAIL POLICY

Reissued March 23, 1998

**UNIVERSITY OF CALIFORNIA
OFFICE OF THE PRESIDENT
ELECTRONIC MAIL POLICY
Reissued March 23, 1998**

TABLE OF CONTENTS

I.	INTRODUCTION	1
	Cautions.....	1
II.	PURPOSE.....	2
III.	DEFINITIONS.....	3
IV.	SCOPE.....	3
V.	GENERAL PROVISIONS.....	4
	A. Purpose	4
	B. University Property	4
	C. Service Restrictions	4
	D. Consent and Compliance	5
	E. Restrictions on Access Without Consent	5
	F. Recourse.....	6
	G. Misuse.....	6
VI.	SPECIFIC PROVISIONS.....	6
	A. Allowable Use	6
	1. Purpose	6
	2. Users.....	6
	3. Non-Competition	7
	4. Restrictions	7
	5. Representation	7
	6. False Identity.....	7
	7. Interference	7
	8. Personal Use.....	7
	B. Security and Confidentiality.....	8
	C. Archiving and Retention	9
VII.	POLICY VIOLATIONS	10
VIII.	RESPONSIBILITY FOR POLICY	10
IX.	CAMPUS RESPONSIBILITIES & DISCRETION	10
	APPENDIX A, DEFINITIONS	12
	APPENDIX B, REFERENCES	15
	APPENDIX C, POLICIES RELATING TO NON-CONSENSUAL ACCESS	17

I. INTRODUCTION

This Policy clarifies the applicability of law and of other University policies to electronic mail. It also defines new policy and procedures where existing policies do not specifically address issues particular to the use of electronic mail.

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. The University affords electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications. This Policy reflects these firmly-held principles within the context of the University's legal and other obligations.

The University encourages the use of electronic mail and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic mail 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 mail services and may inspect, monitor, or disclose electronic mail (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 have taken place; (iii) when there are compelling circumstances as defined in Appendix A; or (iv) under time-dependent, critical operational circumstances as defined in Appendix A, Definitions.

Cautions:

Users should be aware of the following:

1. Both the nature of electronic mail and the public character of the University's business (see Caution 2 below) make electronic mail less private than users may anticipate. For example, electronic mail intended for one person sometimes may 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 "listserver" intended only for the originator of the message may be distributed to all subscribers to the listserver. Furthermore, even after a user deletes an electronic mail record from a computer or electronic mail account it may persist on backup facilities, and thus be subject to disclosure under the provisions of Section V of this Policy. The University cannot routinely protect users against such eventualities.
2. Electronic mail, whether or not created or stored on University equipment, may constitute a University record (see Appendix A, Definitions) subject to disclosure under the California Public Records Act or other laws, or as a result of litigation. However, the University does not automatically comply with all requests for disclosure, but evaluates all such requests

against the precise provisions of the Act, other laws concerning disclosure and privacy, or other applicable law.

Users of University electronic mail services also should be aware that the California Public Records Act and other similar laws jeopardize the ability of the University to guarantee complete protection of *personal* electronic mail resident (see Section VI. A. 8) on University facilities.

The California Public Records Act does not, in general, apply to students except in their capacity, if any, as employees or agents of the University. This exemption does not, however, exclude student email from other aspects of this Policy.

3. The University, in general, cannot and does not wish to be the arbiter of the contents of electronic mail. Neither can the University, in general, protect users from receiving electronic mail they may find offensive. Members of the University community, however, are strongly encouraged to use the same personal and professional courtesies and considerations in electronic mail as they would in other forms of communication.
4. There is no guarantee, unless “authenticated” mail systems are in use, that electronic mail received was in fact sent by the purported sender, since it is relatively straightforward, although a violation of this Policy, for senders to disguise their identity. Furthermore, electronic mail that is forwarded may also be modified. Authentication technology is not widely and systematically in use at the University as of the date of this Policy. As with print documents, in case of doubt receivers of electronic mail messages should check with the purported sender to validate authorship or authenticity.
5. Encryption of electronic mail is another emerging technology that is not in widespread use as of the date of this Policy. This technology enables the encoding of electronic mail so that for all practical purposes it cannot be read by anyone who does not possess the right key. The answers to questions raised by the growing use of these technologies are not now sufficiently understood to warrant the formulation of University policy at this time. Users and operators of electronic mail facilities should be aware, however, that these technologies will become generally available and probably will be increasingly used by members of the community.

II. PURPOSE

The purpose of this Policy is to assure that:

- A. The University community is informed about the applicability of policies and laws to electronic mail;
- B. Electronic mail services are used in compliance with those policies and laws;

-
- C. Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail; and
- D. Disruptions to University electronic mail and other services and activities are minimized.

III. DEFINITIONS

The terms “electronic mail” and “email” are used interchangeably throughout this Policy.

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

- Computing Facility(ies)
- Electronic Mail Systems or Services
- University Email Systems or Services
- Email Record or Email
- University Record
- University Email Record
- Use of University or Other Email Services
- Possession of Email
- Holder of an Email Record or Email Holder
- Faculty
- Substantiated Reason
- Compelling Circumstances
- Emergency Circumstances
- Time-dependent, Critical, Operational Circumstances

IV. SCOPE

This Policy applies to:

- All electronic mail systems and services provided or owned by the University; and
- All users, holders, and uses of University email services; and
- All University email records in the possession of University employees or other email users of electronic mail services provided by the University.

Excluded from the foregoing are electronic mail services of Department of Energy Laboratories managed by the University, and email users of such electronic mail services who are employees and agents of those Laboratories.

This Policy applies only to electronic mail in its electronic form. The Policy does not apply to printed copies of electronic mail. Other University records management policies (see RMP series policies listed in Appendix B, References), however, do not distinguish among the media in which records are generated or stored. Electronic mail messages, therefore, in either their electronic or printed forms, are subject to those other policies, including provisions of those policies regarding retention and disclosure.

This Policy applies equally to transactional information (such as email headers, summaries, addresses, and addressees) associated with email records as it does to the contents of those records.

This Policy is effective immediately, with implementation guidelines to be effective July 1, 1998 (See Section IX).

V. GENERAL PROVISIONS

As noted in the Introduction, the University recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. This Policy reflects these firmly-held principles within the context of the University's legal and other obligations.

- A. **Purpose.** In support of its threefold mission of instruction, research, and public service, the University encourages the use of University electronic mail services to share information, to improve communication, and to exchange ideas.
- B. **University Property.** University electronic mail systems and services are University facilities as that term is used in other policies and guidelines. Any electronic mail address or account associated with the University, or any sub-unit of the University, assigned by the University to individuals, sub-units, or functions of the University, is the property of The Regents of the University of California.
- C. **Service Restrictions.** Those who use University electronic mail services are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of the University, and with normal standards of professional and personal courtesy and conduct. Access to University electronic mail services, when provided, is a privilege that may be wholly or partially restricted by the University without prior notice and without the consent of the email user when required by and consistent with law, when there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to established campuswide procedures or, in the absence of such procedures, to the approval of the appropriate campus Vice Chancellor or University Vice President.

-
- D. **Consent and Compliance.** An email holder's consent shall be sought by the University prior to any inspection, monitoring, or disclosure of University email records in the holder's possession, except as provided for in Section V. E. University employees are, however, expected to comply with University requests for copies of email records in their possession that pertain to the administrative business of the University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by the University. Failure to comply with such requests can lead to the conditions of Section V. E.
- E. **Restrictions on Access Without Consent.** The University shall only permit the inspection, monitoring, or disclosure of electronic mail without the consent of the holder of such email (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 have taken place; (iii) when there are compelling circumstances as defined in Appendix A; or (iv) under time-dependent, critical operational circumstances as defined in Appendix A, Definitions.

When the contents of email 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 Paragraph V.E.2, such actions must be authorized in advance and in writing by the responsible (see Section IX, Campus Responsibilities) campus Vice Chancellor or University Vice President. This authority may not be further re-delegated. Requests for such non-consensual access must be submitted in writing following procedures to be defined by each campus. University counsel's advice shall be sought prior to authorization because of changing interpretations by the courts of laws affecting the privacy of electronic mail, and because of potential conflicts among different applicable laws. Where the inspection, monitoring, or disclosure of email held by faculty is involved, the advice of the Campus Academic Senate shall be sought in writing in advance, following procedures to be established by each campus. All such advice shall be given in a timely manner. 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 V. E. 1 above. If the action taken is not subsequently authorized, the responsible authority shall seek to have the situation restored as closely as possible to that which existed before action was taken.
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 publish, where consistent with law, an annual report summarizing instances of authorized or emergency non-consensual access pursuant to the provisions of this Section.

4. **Compliance with Law.** Actions taken under Paragraphs 1. and 2. shall be in full compliance with the law and other applicable University policy, including laws and policies listed in Appendix B. This has particular significance for email residing on computers not owned or housed by the University. Advice of counsel always must be sought prior to any action taken under such circumstances. It also has particular significance for email whose content is protected under the Federal Family Educational Rights and Privacy Act of 1974, which applies equally to email as it does to print records.
- F. **Recourse.** Procedures for the review and appeal of actions taken under Sections V. C, D, and E and under Section VII shall be implemented (or existing procedures adapted) by each campus 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.
- G. **Misuse.** In general, both law and University policy prohibit the theft or other abuse of computing resources. Such prohibitions apply to electronic mail services and include (but are not limited to) unauthorized entry, use, transfer, and tampering with the accounts and files of others, and interference with the work of others and with other computing facilities. Under certain circumstances, the law contains provisions for felony offenses. Users of electronic mail are encouraged to familiarize themselves with these laws and policies (see Appendix B, References).

VI. SPECIFIC PROVISIONS

A. Allowable Use

In general, use of University electronic mail services is governed by policies that apply to the use of all University facilities. In particular, use of University electronic mail services is encouraged and is allowable subject to the following conditions:

1. **Purpose.** Electronic mail services are to be provided by University organizational units in support of the teaching, research, and public service mission of the University, and the administrative functions that support this mission.
2. **Users.** Users of University electronic mail services are to be limited primarily to University students, faculty, and staff for purposes that conform to the requirements of this Section.

-
3. **Non-Competition.** University electronic mail services shall not be provided in competition with commercial services to individuals or organizations outside the University.
 4. **Restrictions.** University electronic mail services may not be used for: unlawful activities; commercial purposes not under the auspices of the University; personal financial gain (see applicable academic personnel policies); personal use inconsistent with Section VI. A. 8; or uses that violate other University policies or guidelines. The latter include, but are not limited to, policies and guidelines (see Appendix B, References) regarding intellectual property, or regarding sexual or other forms of harassment.
 5. **Representation.** Electronic mail users 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 (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the University¹.
 6. **False Identity.** University email users shall not employ a false identity. Email may, however, be sent anonymously provided this does not violate any law or this or any other University policy, and does not unreasonably interfere with the administrative business of the University.
 7. **Interference.** University email services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of email or email systems.²
 8. **Personal Use.** University electronic mail services may be used 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 operation of computing facilities or electronic mail services; (ii) burden the University with noticeable incremental cost; or (iii) interfere with the email user's employment or other obligations to the University. Email records arising from such personal use may, however, be subject to the presumption in Appendix A, Definition of a University Email Record, regarding personal and other email records. Email users should assess the implications of this presumption in their decision to use University electronic mail services for personal purposes.

¹ An appropriate disclaimer is: "These statements are my own, not those of the University of California."

² Such uses include, but are not limited to, the use of email services to: (i) send or forward email chain letters; (ii) "spam," that is, to exploit listservers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited email; and (iii) "letter-bomb," that is, to resend the same email repeatedly to one or more recipients to interfere with the recipient's use of email.

B. Security and Confidentiality

1. The confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by applicability of law or policy, including this Policy, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorized access. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters.
2. Business and Finance Bulletin RMP-8, *Legal Requirements on Privacy of and Access to Information*, prohibits University employees and others from “seeking out, using, or disclosing” without authorization “personal or confidential” information, and requires employees to take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties or otherwise. This prohibition applies to email records. In this Policy the terms “inspect, monitor, or disclose” are used within the meaning of “seek, use, or disclose” as defined in RMP-8.
3. Notwithstanding the previous paragraph, users should be aware that, during the performance of their duties, network and computer operations personnel and system administrators need from time to time to observe certain transactional addressing information to ensure proper functioning of University email services, and on these and other occasions may inadvertently see the contents of email messages. Except as provided elsewhere in this Policy, they are not permitted to see or read the contents intentionally; to read transactional information where not germane to the foregoing purpose; or disclose or otherwise use what they have seen. One exception, however, is that of systems personnel (such as “postmasters”) who may need to inspect email when re-routing or disposing of otherwise undeliverable email. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt postmasters from the prohibition against disclosure of personal and confidential information of the previous paragraph, except insofar as such disclosure equates with good faith attempts to route the otherwise undeliverable email to the intended recipient. Re-routed mail normally should be accompanied by notification to the recipient that the email has been inspected for such purposes.
4. The University attempts to provide secure and reliable email services. Operators of University electronic mail services are expected to follow sound professional practices in providing for the security of electronic mail records, data, application programs, and system programs under their jurisdiction. Since such professional practices and protections are not foolproof, however, the security and confidentiality of electronic mail cannot be guaranteed. Furthermore, operators of email services have no control over the security of email that has been downloaded to a user’s computer. As a deterrent to potential intruders and to misuse of email, email users should employ whatever protections (such as passwords) are available to them.

-
5. Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies that can be retrieved. Systems may be "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 results in the copying of data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of electronic mail. The practice and frequency of back-ups and the retention of back-up copies of email vary from system to system. Electronic mail users are encouraged to request information on the back-up practices followed by the operators of University electronic mail services, and such operators are required to provide such information upon request.

C. Archiving and Retention

University records management policies do not distinguish among media with regard to the definition of University records. As such, electronic mail records are subject to these policies. In particular, such records are subject to disposition schedules in the University of California Records Disposition Schedules Manual, which distinguishes among different categories of records, from the ephemeral to the archival.

The University does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up (see Section VI. B. 5), 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 mail services are not required by this Policy to retrieve email from such back-up facilities upon the holder's request, although on occasion they may do so as a courtesy.

Email users should be aware that generally it is not possible to assure the longevity of electronic mail records for record-keeping purposes, in part because of the difficulty of guaranteeing that electronic mail can continue to be read in the face of changing formats and technologies and in part because of the changing nature of electronic mail systems. This becomes increasingly difficult as electronic mail encompasses more digital forms, such as embracing compound documents composed of digital voice, music, image, and video in addition to text. Furthermore, in the absence of the use of authentication systems (see Section I, Caution 4), it is difficult to guarantee that email documents have not been altered, intentionally or inadvertently.

Email users and those in possession of University records in the form of electronic mail are cautioned, therefore, to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to transferring (if possible) electronic mail to a more lasting medium/format, such as acid-free paper or microfilm, where long-term accessibility is an issue.

VII. POLICY VIOLATIONS

Violations of University policies governing the use of University electronic mail services may result in restriction of access to University information technology resources. In addition, disciplinary action, up to and including dismissal, may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements.

VIII. RESPONSIBILITY FOR POLICY

The Associate Vice President, Information Resources and Communications (IR&C) in the Office of the President is responsible for development and maintenance of this Policy for issuance by the President.

IX. CAMPUS RESPONSIBILITIES AND DISCRETION

Each Chancellor shall develop, maintain, and publish specific procedures and practices that implement this Policy and communicate its provisions to campus users of University electronic mail services. The following are assigned to individual campus authority and discretion:

- A. Each Chancellor shall decide whether to publish students' electronic mail addresses as directory information. An electronic mail address assigned by the University to a student is a student record, unless assigned in the student's capacity, if any, as an employee or agent of the University. 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 their email addresses public for other than educational purposes.
- B. Each campus shall establish guidelines as to who may use campus electronic mail services, consistent with the provisions of Section VI. A of this Policy.
- C. Each Chancellor shall establish regulations and procedures on actions to be taken once an email user's affiliation with the campus is terminated. In particular, the campus may elect to terminate the individual's email account, redirect electronic mail, or continue the account, subject to the provisions of Section VI. A of this Policy.
- D. Each campus shall establish guidelines and procedures for:

-
1. Restriction of use of University email services pursuant to Section V. C of this Policy;
 2. Authorization, advice, notification, and recourse pursuant to Sections V. E and F of this Policy;
 3. Response to requests for information from users concerning the back-up of electronic mail, pursuant to Section VI. B. 5 of this Policy; and
 4. Any other provisions of this Policy for which procedures are not explicitly stated.
- E. Each Chancellor shall designate the appropriate Vice Chancellor to be responsible for the authorization of action pursuant to Sections V. C and E of this Policy. This authorization responsibility may not be further re-delegated.
- F. Each campus shall establish appropriate notification procedures regarding this Policy to all email users. New users shall positively acknowledge receipt and understanding of the policy. Such notification and acknowledgment may be electronic to the extent that the email user's identity can be assured. It is recognized that it may not be possible to phase in such procedures immediately; however, the lack of comprehensive procedures shall not, in the interim, invalidate the provisions and applicability of this Policy.
- G. Each campus may establish its own procedures that further refine and conform with this Policy.
- H. For purposes of this Section IX, the Office of the President shall be regarded as a campus with respect to its own internal operations, except that for this purpose 'Vice President' shall replace 'Vice Chancellor' in Sections V. C and E.

APPENDIX A DEFINITIONS

Computing Facility(ies): Computing resources, services, and network systems such as computers and computer time, data processing or storage functions, computer systems and services, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation.

Electronic Mail Systems or Services: Any messaging system that depends on computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print computer records for purposes of asynchronous communication across computer network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic mail or is implicitly used for such purposes, including services such as electronic bulletin boards, listservers, and newsgroups.

University Email Systems or Services: Electronic mail systems or services owned or operated by the University or any of its sub-units.

Email Record or Email: Any or several electronic computer records or messages created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several email systems or services. This definition of email records applies equally to the contents of such records and to transactional information associated with such records, such as headers, summaries, addresses, and addressees. This Policy applies only to electronic mail in its electronic form. The Policy does not apply to printed copies of electronic mail.

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 any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained (by the University) regardless of physical form or characteristics. [California Government Code Section 6252(d)]. With certain defined exceptions, such University records are subject to disclosure under the California Public Records Act.

Records held by students, including email, are not University records unless such records are pursuant to an employment or agent relationship the student has or has had with the University. This exemption does not, however, exclude student email from other aspects of this Policy, regardless of whether such email is a University record.

University Email Record: A University Record in the form of an email record regardless of whether any of the computing facilities utilized to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print the email 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 as: (i) a University email record for purposes of this or other University policy (see, however, Sections V. D and E), and (ii) having potential for disclosure under the California Public Records Act.

Until determined otherwise or unless it is clear from the context, any email record residing on university-owned computing facilities may be deemed to be a University email record for purposes of this Policy. This includes, for example, personal email (see Section VI. A. 8). Consistent, however, with the principles asserted in Section V. E. of least perusal and least action necessary and of legal compliance, the University must make a good faith a priori effort to distinguish University email records from personal and other email where relevant to disclosures under the California Public Records Act and other laws, or for other applicable purposes of this Policy.

Use of University or Other Email Services: To create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print email (with the aid of University email services). A (University) Email User is an individual who makes use of (University) email services.

Receipt of email prior to actual viewing is excluded from this definition of “use” to the extent that the recipient does not have advance knowledge of the contents of the email record.

Possession of Email: An individual is in “possession” of an email 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. Thus, an email record that resides on a computer 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 email services are excluded from this definition of possession with regard to email not specifically created by or addressed to them.

Email users are not responsible for email in their possession when they have no knowledge of its existence or contents.

Holder of an Email Record or Email Holder: An email user who is in possession of a particular email record, regardless of whether that email user is the original creator or a recipient of the content of the record.

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

Substantiated Reason: Reliable evidence indicating that violation of law or of policies listed in Appendix C probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

Compelling Circumstances: Circumstances where failure to act may 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, or significant liability to the University or to members of the University community.

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

Time-dependent and Critical Operational Circumstances: Circumstances where 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.

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, however, include all federal and state laws and University policies that may apply to electronic mail. These policies and laws change from time to time; therefore users of this Policy are encouraged to refer to on-line versions of this and other University policies accessible on the Office of the President home page on the World Wide Web.

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, Guidelines for Security of Computing Facilities
- IS-6, Campus Communications Guidelines
- 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 Policies and Agreements:

- Academic Personnel Policy
- Personnel Policies for UC Staff Members (PPSM, current edition)
- Administrative and Professional Staff Program Personnel Policies
- Staff Personnel Policies
- 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
- University of California Records Disposition Schedules Manual
- University Policy on Integrity in Research

State of California Statutes

State of California Education Code, Section 67100 et seq.

State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)

State of California Public Records Act (Gov. Code Section 6250 et seq.)

State of California Penal Code, Section 502

Federal Statutes

Federal Family Educational Rights and Privacy Act of 1974

Federal Privacy Act of 1974

Electronic Communications Privacy Act of 1986

APPENDIX C

POLICIES RELATING TO NON-CONSENSUAL ACCESS

This University Electronic Mail Policy references circumstances where access to electronic mail may occur without the prior consent of the holder (see I. Introduction and Section V.E). Following is the list of University policies that may trigger such non-consensual access following procedures defined in Section V.E.2.

1. Policies governing sexual or other forms of harassment, specifically: Section APM-035, Appendix A of the Faculty Code of Conduct; Personnel Policies for UC Staff Members; Administrative and Professional Staff Program Personnel Policies, Sections 112.1 and 112.2; Staff Personnel Policies, Section 200.2. (For exclusively represented employees in units where initial collective bargaining agreements are under negotiation, applicable personnel policies continue to govern until an agreement is concluded.) Sexual harassment by 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 VIIG; 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. University of California Personnel Policies for Staff Members, Administrative and Professional Staff Program Personnel Policies and Staff Personnel Policies. (For exclusively represented employees in units where initial collective bargaining agreements are under negotiation, applicable personnel policies continue to govern until an agreement is concluded.)
5. All 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 V and VI of this Electronic Mail Policy.

Violations of other policies can normally be detected and investigated without requiring non-consensual access to electronic mail. However, on occasion attention to possible policy violations is brought about because of the receipt by others of electronic mail. Electronic mail, however can be forged; the true identity of the sender can be masked; and the apparent sender may deny authorship of the electronic mail. 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 mail may be authorized following the procedures defined in Section V.2, 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 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.