

Electronic Communications Policy

Attachment 1 User Advisories

University of California
Office of the President

Issued November 17, 2000

Updated January 14, 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.	ARCHIVING	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 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 ~~web pages~~ **electronic communications resources**, users create transaction records that leave a trail of the ~~web pages visited~~ **electronic communications resources used** and might give ~~the web host~~ information about the users **and their activities**. Current state and federal laws governing such electronic data gathering ~~are insufficient to~~ **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 their disclosure and privacy policies.**

VI. SECURITY CONSIDERATIONS

A. SECURITY

~~Encryption of electronic communications is an emerging technology that is in limited use at the present time. This~~ **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 ~~right key~~ **commensurate technology needed to decrypt them**. Users of electronic communications should be aware that the University does not routinely encrypt electronic communications ~~on~~ **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

~~Some~~ Electronic communications systems (~~including some voicemail 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. ARCHIVING

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 to a more lasting medium or format, such as acid-free paper or microfilm, for long-term accessibility as required.