SAN JOSE STATE
UNIVERSITY

A campus of The California State University

Office of the Academic Senate • One Washington Square • San Jose, California 95192-0024 • 408-924-2440 • Fax: 408-924-2410

F97-7

At its meeting of December 1, 1997, the Academic Senate approved the following policy recommendation presented by David McNeil for the Professional Standards Committee.

POLICY RECOMMENDATION
PRIVACY OF ELECTRONIC INFORMATION AND COMMUNICATIONS

WHEREAS: San Jose State University, along with its faculty, staff, and students, relies heavily on the electronic transmission of communications and storage of data; and

WHEREAS: The nature of electronic information and communications technology is such that questions of privacy and security are associated with its use; therefore, be it

RESOLVED: That the following policy be implemented.

ACTION BY THE UNIVERSITY PRESIDENT

Approved
12-17-97

PRIVACY OF ELECTRONIC INFORMATION AND COMMUNICATIONS

The privacy of personal and professional communications and stored information is a matter of concern in an era when the speed, capacity, and complexity of communications and information technologies are greatly expanding. The faculty, staff, and students of San Jose State University require and deserve a reasonable degree of assurance that their e-mail, telephone calls, voice mail, or other communications, research data, academic writing, and other electronic information are transmitted and stored on University facilities with an appropriate degree of privacy and security. No electronic system is entirely secure from unauthorized intrusions, and users are to be warned that electronic communications and information can be easily accessed by third parties. Systems administrators may inspect stored data on occasions when the integrity of the system may be jeopardized, or pursuant to legal requirements, including disclosure under the Public Records Act, discovery in civil litigation, and legal searches performed in cooperation with state and federal law enforcement authorities. Because of uncertainty about who may inspect electronic files and under what circumstances, principles concerning approved access to electronic information need to be adopted as policy and distributed to all campus users of electronic communication and information storage.

San Jose State University supports privacy in the use of electronic communications and information storage to the maximum extent possible under state and federal laws, consistent with computer system maintenance demands. Users of campus computing facilities are expected to use them appropriately for professional and non-commercial purposes. In general, communications and other information transmitted or stored on campus computing facilities are the property of their authors and intended recipients, and no third party other than the creator or designated recipient is authorized to intercept such information or communications, except that inspections of electronic mail may occur for the purpose of technical problem resolution, if approved by the user or the appropriate computer affairs administrator or supervisor for the resolution of a specific technical problem or suspected misuse that is believed to endanger the integrity of the computer system. All electronic mail and files in authorized accounts stored on any campus computing systems shall be considered to be private and confidential, except as required by state or federal law.

The Chief Information Officer shall be responsible for implementation of this policy. Each systems administrator for each campus electronic information or communications system should, in coordination with the Chief Information Officer, create guidelines for the privacy of electronic information and communications.

SAN JOSÉ STATE UNIVERSITY
ONE WASHINGTON SQUARE
SAN JOSÉ, CA 95192

S17-8, University Policy, Privacy of Electronic Information

Legislative History:

At its meeting of April 10, 2017, the Academic Senate approved the following policy recommendation presented by Senator Peter for the Professional Standards Committee. This document explains the rationale for protecting privacy of electronic information within the context of academic freedom and the culture of a university of higher learning, and summarizes important principles on privacy of electronic information as found in the AAUP document "Academic Freedom and Electronic Communications" and elements of the University of California system policy on "Electronic Communications."

Rescinds and Replaces: F97-7

Effective: Immediately

Signed (date):_____

Approved by:_____

Mary A. Papazian, President, San José State University

University Policy
Privacy of Electronic Information

Resolved: That F97-7 be rescinded.

Resolved: That the following be adopted as policy effective immediately.

Rationale: This document summarizes important principles on privacy of electronic information found in the AAUP document "Academic Freedom and Electronic Communications" and elements copied from the University of California system policy on "Electronic Communications." Our archaic F97-7 was very vague and increasingly obsolete. The CSU system policy has some useful protections, but does not directly address information privacy in a forthright manner. This document explains the

rationale for protecting privacy of electronic information within the context of academic freedom and the culture of a university of higher learning.

While Professional Standards originally created a bulkier and considerably more specific policy draft, negotiations with the President's Chief of Staff and the Information Security Officer persuaded us to slim the policy down to key principles and leave the minutiae to a Presidential Directive that is currently under draft.

Approved:	*April 3, 2017*
Vote:	*9-0-0*
Present:	*Peter, Green, White, Lee, Reade, Kauppila, Hamedi-Hagh, Hwang, Marachi*
Absent:	*Caesar*
Financial Impact:	*No direct impacts*
Workload Impact:	*No direct impacts*

POLICY RECOMMENDATION
Principles Regarding Privacy of Electronic Information

1. Purpose

   1.1. San José State University (SJSU) recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications.
   1.2. SJSU 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.
   1.3. SJSU recognizes the value of privacy as a condition for academic freedom and the benefits that privacy and autonomy bring to the individual, to groups, and to the culture of SJSU.
   1.4. SJSU recognizes that faculty members and students have a reasonable expectation of privacy in their electronic communications.
   1.5. San Jose Staté University supports privacy in the use of electronic communications and information storage to the maximum extent possible under state and federal laws.

2. Principles governing involuntary disclosure
   2.1. ***Rarely used and clearly defined***. SJSU does not examine or disclose the contents of electronic records without the consent of the individual participating in the communication except in rare cases that are clearly defined.
   2.2. ***Clear authorization.*** When involuntary disclosure takes place, it must first be authorized by the President, and records of the authorization must be kept.
   2.3. ***Least Perusal.*** Authorization shall be limited to the least perusal of contents and the least action necessary to resolve a matter.
   2.4. ***Disclosure.*** SJSU shall at the earliest opportunity that is lawful and consistent with other University policy notify the affected individual of the action(s) taken and the reasons for the action(s) taken.
   2.5. ***Institutional Accountability.*** In a manner consistent with law and concerns of confidentiality, SJSU shall prepare an annual report tracking the frequency and general purpose of all authorizations of involuntary disclosure. This report will be circulated to an appropriate body of stakeholders that will include tenured faculty chosen by the Academic Senate.

3. Implementation

The President will issue and maintain a directive that implements the purpose and principles of this policy

4. Privacy Advisory

Various laws and available security technologies affect the degree of privacy that users can expect. No electronic system is entirely secure from unauthorized intrusions. Users should be warned that legal requirements may require disclosure, such as disclosure under the Public Records Act, discovery in civil litigation, and legal searches performed in cooperation with state and federal law enforcement authorities.

SJSU SAN JOSÉ STATE UNIVERSITY

Mary A. Papazian, Ph.D.
President

San José State University
One Washington Square
San José, CA 95192-0002

TEL: 408-924-1177
FAX: 408-924-1199
sjsupres@sjsu.edu

The California State University:
Chancellor's Office
Bakersfield
Channel Islands
Chico
Dominguez Hills
East Bay
Fresno
Fullerton
Humboldt
Long Beach
Los Angeles
Maritime Academy
Monterey Bay
Northridge
Pomona
Sacramento
San Bernardino
San Diego
San Francisco
San José
San Luis Obispo
San Marcos
Sonoma
Stanislaus

April 20, 2018

To: Academic Senate Executive Committee

From: Mary A. Papazian, Ph.D.

Re: Policy Rescinding and Replacing F97-7 Policy on Privacy of Electronic Information (S17-8).

On April 3, 2017, the Academic Senate approved a draft policy to rescind and replace the existing F97-7 Policy on Privacy of Electronic Information. I am declining to approve the draft policy as written, primarily because the CSU has an approved "Responsible Use Policy" for Information Technology that in my view provides much of the appropriate framework for addressing questions related to the privacy of electronic information and our various employee groups are covered by collective bargaining agreements that provide protections on due process and disciplinary action.

The policy approved by the Academic Senate divides into four sections:

- Purpose
- Principles governing involuntary disclosure
- Implementation
- Privacy Advisory

The section on Purpose reads more like a section of Principles. I am comfortable with this section with the edits below:

1. acceptable as written
2. acceptable as written
3. replace "a condition for" with "part of" to read: "SJSU recognizes the value of privacy as *part of* academic freedom and the benefits that privacy and autonomy bring to the individual, to groups, and to the culture of SJSU.
4. replace "have a reasonable expectation of privacy" (which has legal connotations) with language similar to the CSU policy to read: "SJSU respects the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers, graphics and videos.
5. replace "under" with "in accordance with CSU policy" to read "San Jose State University supports privacy in the use of electronic communications and information storage to the maximum extent possible *in accordance with CSU policy*, state and federal laws, and consistent with computer system maintenance demands.

I am not inclined to approve a policy with the language in section 2. The statements are directives and address specific implementation areas. The statements made in Section 1 set forth the principles upon which implementation will take place.

Regarding Section 3, I am happy to discuss further the implementation of the campus policy statement via Presidential Directive.

I also am comfortable with the language in section 4, "Privacy Advisory" with the following addition in the last sentence "...may require disclosure, including but not limited to, disclosure under the Public records Act..."

Please let me know if you have any questions regarding my response. I would be glad to discuss further.

Electronic Communications Policy

University of California
Office of the President

Issued November 17, 2000
Revised August 18, 2005

TABLE OF CONTENTS

I. INTRODUCTION

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

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

II. GENERAL PROVISIONS

A. PURPOSE

The purposes of this Policy are to:

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

B. SCOPE

This Policy applies to:

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

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

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

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

C. DEFINITIONS

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

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

D. RESPONSIBILITIES

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

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

3. **Informational Material.** Campuses shall provide users of University electronic communications resources with instructional material based on this Policy and on their own campus implementation guidelines.

E. VIOLATIONS OF LAW AND POLICY

1. **Law.** Federal and state law prohibit the theft or abuse of computers and other electronic resources such as electronic communications resources, systems, and services. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of electronic communications resources, systems, and services. The law classifies certain types of offenses as felonies (see Appendix B, References).

2. **University Disciplinary Actions.** University policy prohibits the use of University property for illegal purposes and for purposes not in support of the mission of the University. In addition to legal sanctions, violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to University policies and collective bargaining agreements. Further information on permitted and prohibited uses is given in Section III, Allowable Use.

III. ALLOWABLE USE

A. INTRODUCTION

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

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

B. OWNERSHIP

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

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

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

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

C. ALLOWABLE USERS

1. **University Users.** University students, faculty, staff, and others affiliated with the University (including those in program, contract, or license relationships with the University) may, as authorized by the Chancellor, be eligible to use University electronic communications resources and services for purposes in accordance with Sections III.D, Allowable Use.

2. **Public Users**. Persons and organizations that are not University Users may only access University electronic communications resources or services under programs sponsored by the University, as authorized by the Chancellor, or for the Office of the President, the Senior Vice President, Business and Finance, for purposes of such public access in accordance with Section III.D, Allowable Use.

3. **Transient Users.** Users whose electronic communications merely transit University facilities as a result of network routing protocols are not considered "Users" for the purposes of this Policy.

D. ALLOWABLE USES

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

1. **Purpose.** Electronic communications resources may be provided by University units or sub-units in support of the teaching, research, and public service mission of the University, and of the administrative functions that support this mission.

2. **Non-Competition.** University electronic communications resources shall not be provided to individual consumers or organizations outside the University except by approval of the Chancellor. Such services shall support the mission of the University and not be in competition with commercial providers.

3. **Restrictions.** University electronic communications resources may not be used for:

- unlawful activities;
- commercial purposes not under the auspices of the University;
- personal financial gain (except as permitted under applicable academic personnel policies);
- personal use inconsistent with Section III.D, Allowable Uses; or
- uses that violate other University or campus policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property and sexual or other forms of harassment (see Appendix B, References).

4. **Representation.** Use of the University's name and seal is regulated by the State of California Education Code 92000. Users of electronic communications resources must abide by this statute as well as by University and campus policies on the use of the University's name, seals, and trademarks (see Appendix B, References). Users of electronic communications resources shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized to do so.

5. **Endorsements**. Users of electronic communications resources must abide by University and campus policies regarding endorsements. References or pointers to any non-University entity contained in University electronic communications shall not imply University endorsement of the products or services of that entity.

6. **False Identity and Anonymity.** Users of University electronic communications resources shall not, either directly or by implication, employ a *false identity* (the name or electronic identification of another). However, when not prohibited by law or other University policy, a supervisor may direct an employee to use the supervisor's identity to transact University business for which the supervisor is responsible. In such cases, an employee's use of the supervisor's electronic identity does not constitute a false identity.

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

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

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

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

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

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

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

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

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

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

E. ACCESS RESTRICTION

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

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

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

IV. PRIVACY AND CONFIDENTIALITY

A. INTRODUCTION

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications. This Policy reflects these firmly-held principles within the context of the University's legal and other obligations. The University respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations, while seeking to ensure that University administrative records are accessible for the conduct of the University's business.

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

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

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

B. ACCESS WITHOUT CONSENT

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

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

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

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

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

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

2. **Emergency Circumstances**. In emergency circumstances as defined in Appendix A, Definitions, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described in Section IV.B.1, Authorization, above.

3. **Notification.** The responsible authority or designee shall at the earliest opportunity that is lawful and consistent with other University policy notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

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

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

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

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

5. **Recourse.** Campus implementing procedures shall specify the process for review and appeal of actions taken under Sections IV.B.1, Authorization, and IV.B.2, Emergency Circumstances to provide a mechanism for recourse to individuals who believe that actions taken by employees or agents of the University were in violation of this Policy.

6. **Search Warrants and Subpoenas.** Search warrants and subpoenas are not subject to sections 1-2 and 4-5 above. Search warrants and subpoenas for electronic communications records shall be referred to University legal counsel at the Office of the General Counsel or designated officials at campus locations.

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

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

C. PRIVACY PROTECTIONS AND LIMITS

1. Privacy Protections

a. Personal Information. Federal and California law provide privacy protections for some information that personally identifies an individual. Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information, provides guidelines for the collection and use of personal information in conformance with the law. These guidelines apply to information collected and disseminated by electronic means just as they do to records stored on paper and other media.

b. Student Information. Users of electronic communications systems and services shall not disclose information about students in violation of the federal Family Educational Rights and Privacy Act of 1974 (FERPA), and the University policies that provide guidance in meeting FERPA requirements. See Business and Finance Bulletin RMP-8, Legal

Requirements on Privacy of and Access to Information, and the University's Policy Applying to the Disclosure of Information from Student Records (Sections 130-134 of the Policies Applying to Campus Activities, Organizations, and Students).

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

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

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

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

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

2. Privacy Limits

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

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

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

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

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

V. SECURITY

A. INTRODUCTION

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

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

B. SECURITY PRACTICES

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

C. INTEGRITY

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

D. AUTHENTICATION

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

E. AUTHORIZATION

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

F. ENCRYPTION

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

G. RECOVERY

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

H. AUDIT

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

VI. RETENTION AND DISPOSITION

A. RETENTION

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

B. DISPOSITION

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

C. BACK-UP

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

APPENDIX A: DEFINITIONS

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

Electronic Communications: Any transfer of signals, writings, images, sounds, data or intelligence that is, created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems[2]. For purposes of this Policy, an electronic file that has not been transmitted is not an electronic communication.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

APPENDIX B: REFERENCES

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

University Policies and Guidelines

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

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

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

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

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

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

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

State of California Statutes

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

Federal Statutes and Regulations

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

APPENDIX C: POLICIES RELATING TO ACCESS WITHOUT CONSENT

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

1. University policies governing sexual or other forms of harassment, specifically: Policies Applying to Campus Activities, Organizations, and Students, Section 160; Section APM-035, Appendix A of Affirmative Action and Nondiscrimination in Employment; and Personnel Policies for UC Staff Members. Sexual harassment concerning students is covered by item 6 below.

2. Certain portions of policies governing access to University records, specifically RMP-1, Section IV.B; RMP-8, Sections on Disclosure of Information and Rules of Conduct.

3. The Academic Personnel Manual, APM-015, Section II, Part II, Professional Responsibilities, Ethical Principles, and Unacceptable Faculty Conduct, and the University Policy on Integrity in Research, APM 190, Appendix B.

4. Personnel Policies for Staff Members and Appendix II for Senior Managers

5. Collective bargaining agreements and memoranda of understanding.

6. Section 102 governing student conduct of the policy entitled Policies Applying to Campus Activities, Organizations, and Students.

7. Sections III, Allowable Use, and IV, Privacy and Confidentiality, of this Electronic Communications Policy.

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

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

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

Posting and Authority to Change

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

ECP SUPPORTING DOCUMENTS

Attachment 1 User Advisories

Attachment 2 Implementation Guidelines

Electronic Communications Policy

Attachment 1
User Advisories

University of California
Office of the President

Issued November 17, 2000
Revised August 18, 2005

TABLE OF CONTENTS

I. INTRODUCTION

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

II. USER RESPONSIBILITIES

A. COMPLIANCE WITH LAW

The Electronic Communications Policy refers to federal laws that prohibit:

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

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

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

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

B. ALLOWABLE USES

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

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

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

C. COURTESY

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

III. PRIVACY EXPECTATIONS

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

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

- Users generally expect a high level of privacy with telephone conversations, and these expectations are generally protected by law;

- Users often expect a similarly high level of privacy with electronic mail, but (i) these expectations are not always supported by law, and (ii) recipients may compromise confidentiality by redirecting electronic mail messages;

- Users might expect a more moderate level of privacy with electronic communications intended for distribution to a limited audience, since privacy can be compromised by the limit of available security protections or by the behavior

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

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

IV. PRIVACY PROTECTIONS

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

A. PERSONAL INFORMATION

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

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

B. STUDENT PRIVACY

Federal law protecting student privacy is incorporated into University policies. In accordance with the policies and procedures in the University's Policy Applying to the Disclosure of Information from Student Records (Sections 130-134 of the Policies Applying to Campus Activities, Organizations, and Students), campuses are responsible for designating the categories of personally identifiable information about a student that are public. Individual students may, consistent with the above policy, request the campus not to make public their electronic mail addresses and telephone numbers (see Electronic Communications Policy, Section II.D, Responsibilities and Section IV.C, Privacy Protections and Limits).

C. ELECTRONIC DATA GATHERING

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

V. PRIVACY LIMITS

A. INTRODUCTION

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

B. PUBLIC RECORDS

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

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

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

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

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

C. UNIVERSITY POLICIES

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

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

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

D. UNINTENDED DISTRIBUTION

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

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

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

E. ELECTRONIC DATA GATHERING

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

VI. SECURITY CONSIDERATIONS

A. SECURITY

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

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

B. AUTHENTICATION

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

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

C. BACK-UP

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

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

D. DISPOSITION

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

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

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

Electronic Communications Policy

Attachment 2
Implementation Guidelines

University of California
Office of the President

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

TABLE OF CONTENTS

I. INTRODUCTION

A. PURPOSE

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

B. CAMPUS RESPONSIBILITIES

Campuses shall develop guidelines and procedures in accordance with these Implementation Guidelines in consultation with campus faculty, students, and staff.

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

2. Each Chancellor shall establish guidelines as to who may use the electronic communications resources under that Chancellor's jurisdiction, consistent with provisions of Policy Section III.C, Allowable Users.

3. Each Chancellor shall establish regulations and procedures on actions to be taken once a user's affiliation with the campus is terminated. In particular, the campus may elect to terminate the individual's access, redirect electronic communications, or continue the access, subject to provisions of Policy Section III.C, Allowable Users, and consistent with Business and Finance Bulletin IS-3, Electronic Information Security.

4. Each Chancellor shall establish guidelines and procedures for:

    - Restricting or denying the use of University electronic communications resources in accordance with Policy Section III.E, Access Restriction;

    - Authorization, advice, notification, and recourse as required by Policy Section IV.B, Access Without Consent; and

    - Response to user requests for information about the back-up of electronic communications, as required by Policy Section IV.C, Privacy Protections and Limits.

5. Each Chancellor shall designate the appropriate Vice Chancellor(s) to authorize action pursuant to Policy Sections III.D, Access Restriction, and IV.B, Access Without Consent. The authority for access without consent may not be further re-delegated.

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

6. Each Chancellor shall establish procedures for responding promptly to allegations regarding copyright infringement, sexual or other forms of harassment, defamation, and other violations arising from electronic communications where the University might be responsible for mitigation (see Electronic Communications Policy, Section III.E, Access Restriction).

7. Each Chancellor may establish campus guidelines covering:

   - Procedures for reimbursement of incremental costs incurred for incidental personal use of University electronic communications resources (see Electronic Communications Policy Section III.D, Allowable Uses);
   - Establishment of web pages, mailing list systems, newsgroups and bulletin boards for personal use on University electronic communications resources;
   - Procedures for identifying official University web pages; and
   - Methods for billing residence hall telephone systems.

8. In accordance with the policies and procedures in the University's Policy Applying to the Disclosure of Information from Student Records (Sections 130-134 of the Policies Applying to Campus Activities, Organizations, and Students), each Chancellor shall designate the categories of personally identifiable information about a student that are public and shall establish procedures by which individual students may request that the campus not make public their electronic mail addresses and telephone numbers (see Electronic Communications Policy Section IV.C.1, Privacy Protections).

9. Each Chancellor may establish additional procedures that further refine and conform with this Policy.

10. For purposes of this Policy, the Office of the President shall be regarded as a campus with respect to its own internal operations.

II. ALLOWABLE USE

A. ALLOWABLE USERS

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

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

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

B. ALLOWABLE USES

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

2. **Endorsements.** When an electronic communication might give the impression that the author's endorsement represents an endorsement by the

University, the communication must include an explicit disclaimer. Campus guidelines should provide means of meeting this requirement concerning implied endorsements. Among other alternatives, they may: i) provide specifications for a context that makes a disclaimer unnecessary for a particular electronic communications service; ii) provide for a common disclaimer that can be shared by users of an electronic communications service; or iii) suggest the wording of a disclaimer to be included by the author, e.g. "References or pointers to non-University entities do not represent endorsement by the Regents of the University of California."

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

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

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

4. **Interference.** Campus guidelines should identify examples of behaviors that are likely to interfere with the operation of University electronic communications resources so users can, in good faith, avoid them. Guidelines should clarify that additional behaviors may also prove to be disruptive, since technological advances may lead to new abuses of electronic communications resources. Guidelines should also distinguish between behaviors that are purposeful and those that cause unintended disruption of services.

5. **Personal Use.** Campus implementing guidelines may specify terms and conditions for the personal use of specific electronic communications services, consistent with the provisions for personal use in Policy Section III.D.8.

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

   Users should be encouraged to avoid noticeable incremental charges to the University for personal use of University facilities by employing telephone cards, private email accounts, and other mechanisms to charge such costs to personal accounts. When personal use causes noticeable incremental costs to

the University, users shall reimburse the University following campus procedures and guidelines (see Electronic Communications Policy Section III.D.8, Personal Use and Responsibilities above).

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

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

C. ACCESS RESTRICTION

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

D. USE OF SPECIFIC SERVICES

1. Web Pages

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

a. Identification. Web pages shall not be posted anonymously at addresses within a University domain (i.e., campus.edu). Campus guidelines may establish local standards for identifying the University unit, sub-unit, program, or individual responsible for the page.

b. Official University Web Pages. The Chancellor shall determine what rules to apply to web pages in order to comply with provisions of Policy Sections III.D. 4 and 5, Representation and Endorsement. For this purpose, the Chancellor may designate certain web pages as official University web pages. Conversely, the Chancellor may designate mechanisms for identifying personal web pages that do not represent the University. Any identification used to denote official web pages must not be used for other web pages.

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

2. Radio Frequency Stations

a. **Station Licenses**. Operation of radio frequency stations (including television, radio, auxiliary broadcast facilities, maritime, aeronautical, land mobile, satellite, microwave, and paging) requires Federal Communications Commission licensing. Campuses shall apply for such licenses through the Office of the Associate Vice President, Information Resources and Communications.

b. **Radio Frequency Interference**. Users of telecommunications radio frequency transmitters and receivers shall operate such equipment in compliance with regulations of the Federal Communications Commission. In particular, users shall not interfere with other station operators or other users on the same station, regardless of whether such operators or users are affiliated with the University.

III. PRIVACY AND CONFIDENTIALITY

A. ACCESS WITHOUT CONSENT

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

1. **Authorization.** Campus procedures for authorization to access electronic communications without consent shall include the following requirements:

   - Requests for nonconsensual access must be submitted in writing except in emergency circumstances. In accordance with Policy Section IV.B.2, Emergency Circumstances, actions must be limited to the least perusal of contents and the least action necessary to resolve the emergency. Appropriate written authorization must subsequently be sought without delay.

   - Advice of campus legal counsel or an attorney in the Office of General Counsel shall be sought prior to authorization of nonconsensual access. Counsel's advice shall be sought in the event of receipt of legal documents demanding information, such as search warrant, subpoena, or subpoena duces tecum, in accordance with Policy Section IV.B, Access without Consent, RMP-10, Instructions for Responding to Subpoena, and campus implementing procedures.

2. **Procedures concerning faculty**. Chancellors shall confer with their respective Divisional Senate to establish procedures for nonconsensual access to electronic communications where the examination or disclosure involves electronic communications held by faculty.

3. **Notification.** Advice of legal counsel shall be sought in determining whether there is reason not to notify an individual that his or her electronic communications have been accessed without consent.

4. **Annual Report.** Each Chancellor shall annually report to the Office of Information Resources and Communications in the Office of the President the number of cases of nonconsensual access to electronic communications that have taken place. The annual report will identify the:

   - Number of requests for nonconsensual access,
   - Number of requests granted on emergency basis,
   - Number of requests granted after prior approval,
   - Number of requests denied, and
   - Reasons for requests: (i) Required by and consistent with law, (ii) Substantiated reason to believe that violations of law or University policies have taken place, (iii) Compelling circumstances, and/or (iv) Time-dependent, critical operational circumstances.

   Annual reports shall consist of summary numbers with no information about individual cases, and shall be posted on the web so the data will be available to the University community and the public. Access that results from search

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

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

B. PRIVACY PROTECTIONS AND LIMITS

1. **Personal Information.** A written release should be obtained prior to posting, broadcasting, or distributing an individual's picture or statement, except in cases of news reporting.

2. **Student Information.** Campus guidelines should clarify what student information may and may not be released, consistent with Policy Section IV.C.1.b, Student Information, and Responsibilities I.B.g. above.

3. **Electronically Gathered Data.** When a University electronic communications service automatically collects information about a user (for instance, through cookies and banner ads), notice to that effect should be posted at the beginning of the transaction and should indicate what information will be collected and how it will be used. Ideally, users should be allowed to terminate the transaction at that point without leaving data behind.

4. **System Monitoring.** Campus guidelines shall ensure that University personnel who operate and support electronic communications resources understand and comply with the provisions of Policy Section IV.C.2.b, System Monitoring, regarding the conditions under which they may observe the contents of electronic communications or transactional information. This section of the Policy also requires that they not disclose the contents of communications they have observed, except as required by law or policy. Providers of electronic communications services shall document and make available general information about the monitoring practices of systems under their control consistent with Policy Section V.B. Security Practices. This information shall include types of monitoring activities, the level of inspection required to examine suspect electronic communications records, and accompanying procedures. This information serves to meet the ECP provision requiring the documentation of routine monitoring practices.

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

nonconsensual access (see Electronic Communications Policy Sections III.D.7, Interference, IV.C.2.b, System Monitoring, and V.A., Security).

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

a. Absences. In order to reduce the need to access an employee's electronic communications records in the event of absence, campuses are encouraged to use techniques or procedures to minimize the need to gain access without consent. Following are some practices that campuses may implement.

- *"Absence" messages*. Include in procedures the requirement that absence messages be installed to indicate the period of time of absence and alternate contact information.
- *Email forwarding*. Use email forwarding capabilities, if available, so that during planned absences electronic communications will be forwarded to authorized individual(s).
- *Workgroup accounts*. Establish common workgroup accounts for department-related business so essential departmental business electronic communications are accessible to all workgroup members.
- *Autoforwarding with Filtering*. Set filters to forward selected electronic communications to relevant staff in the holder's absence.
- *Mailing lists*. Establish mailing lists so that all subscribers receive a copy of any messages posted to the list.
- *Shared files*. Establish file server capability to store and access documents in support of business operations. Authorization and access procedures must be clearly documented.

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

b. Separated Employees. Appropriate campus guidelines shall include recommendations for exit procedures that include clear instructions regarding the disposition of employee electronic communications records subsequent to the employee's separation from the University. Employees shall be informed of these procedures upon employment.

Exit procedures shall include:

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

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

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

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

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

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

C. PRIVACY OF SPECIFIC SERVICES

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

Academic Freedom and Electronic Communications

This report was prepared by a subcommittee of the Association's Committee A on Academic Freedom and Tenure and initially published in 1997. A revised text was approved by Committee A and adopted by the Association's Council in November 2004. A revised and expanded text was approved by Committee A and adopted by the Association's Council in November 2013.

In November 2004, the Association's Council adopted *Academic Freedom and Electronic Communications*,[1] a report prepared by a subcommittee of Committee A on Academic Freedom and Tenure and approved by Committee A. That report affirmed one "overriding principle":

> Academic freedom, free inquiry, and freedom of expression within the academic community may be limited to no greater extent in electronic format than they are in print, save for the most unusual situation where the very nature of the medium itself might warrant unusual restrictions—and even then only to the extent that such differences demand exceptions or variations. Such obvious differences between old and new media as the vastly greater speed of digital communication, and the far wider audiences that electronic messages may reach, would not, for example, warrant any relaxation of the rigorous precepts of academic freedom.

This fundamental principle still applies, but developments since publication of the 2004 report suggest that a fresh review of issues raised by the continuing growth and transformation of electronic-communications technologies and the evolution of law in this area is appropriate. For instance, the 2004 report focused largely on issues associated with e-mail communications and the posting of materials on websites, online bulletin boards, learning-management systems, blogs, and listservs. Since then, new social media, such as Facebook, LinkedIn, Reddit, Tumblr, and Twitter, have emerged as important vehicles for electronic communication in the academy.

Already in 2004 it was clear that electronic communications could easily be forwarded to others at vastly greater speeds, with potentially profound implications for both privacy and free expression. As Robert M. O'Neil has written, "An electronic message may instantly reach readers across the country and indeed around the globe, in sharp contrast to any form of print communication. Although a digital message, once posted, can be infinitely altered over time—another significant difference—the initial message may never be retracted once it has been sent or posted. Indeed, the first posting may remain accessible on 'mirror' sites despite all efforts to suppress, remove, and expunge it."[2] Electronic communications can be altered, or presented selectively, such that they are decontextualized and take on implicit meanings different from their author's original intent. With the advent of social media such concerns about the widespread circulation and compromised integrity of communications that in print might have been essentially private have only multiplied further.

Moreover, while the 2004 report assumed that electronic communications produced by faculty members in the course of their teaching and research were physically located on servers and computers owned and operated by their colleges and universities, today institutions increasingly employ technologies associated with cloud computing and other outsourcing strategies. These may involve relinquishing control to third-party services, storing data at multiple sites administered by several organizations, and relying on multiple services across the network—a shift that poses potentially profound challenges to academic freedom.

These changes have been magnified by the growing proliferation of new electronic-communications devices, such as smartphones and tablets. At Oakland University in Michigan, for example, the university's roughly 7,500 students now bring an average of 2.5 devices each to campus, while faculty members bring about two.[3] The desire of growing numbers of faculty members, staff members, and students to have access to communications and information on multiple devices, especially mobile devices, has increasingly driven institutions to create "BYOD"

(bring-your-own-device) policies. By embracing individual consumer devices, an institution may better address the personal preferences of its faculty, staff, and students, offering not only increased mobility but also increased integration of their personal, work, and study lives. However, the increasing number of devices and the increasing demand for bandwidth from new applications may strain institutional resources in ways that might lead institutions to establish access restrictions that could adversely affect academic freedom.

More important, such practices can further blur boundaries between communications activities that are primarily extramural or personal and those that are related more directly to teaching and scholarship. Digital devices such as smartphones have also promoted increased interactivity between users and their devices, permitting users to create their own content but also to leave personal "footprints," which might be subject to surveillance.

As in 2004, "college and university policies that were developed for print and telephonic communications"—and policies developed for earlier modes of electronic communications—"may simply not fit (or may fit imperfectly) the new environment." *Faculty members need to understand more completely the implications for academic freedom of electronic-communications technologies, and they should be directly involved in the formulation and implementation of policies governing such technology usage.*

I. Freedom of Research and Publication

The 2004 report affirmed: "The basic precept in the 1940 *Statement of Principles on Academic Freedom and Tenure* that 'teachers are entitled to full freedom in research and in the publication of the results' applies with no less force to the use of electronic media for the conduct of research and the dissemination of findings and results than it applies to the use of more traditional media." As that report noted, however, access to materials in digital format may be subject to greater restrictions than would be the case with print-format materials.

A. Access to Information in Digital Format

Academic freedom is dependent on a researcher's ability not only to gain access to information but also to explore ideas and knowledge without fear of surveillance or interference. Historically, scholars have gained access to published and often to unpublished research materials through college and university libraries. Electronic-communications technologies have permitted many libraries to offer access to a far broader array of materials than in the past through a wide variety of online databases. Some online catalogs, designed to replicate social media, now allow users to leave notations and reviews of cataloged materials that can be viewed around the world.

To be sure, as O'Neil has noted, "[a]lthough a university does to some degree control a scholar's recourse to print materials by its management of library collections, . . . the potential for limitation or denial of access is vastly greater when the institution maintains and therefore controls the gateway to the Internet."[4] Colleges and universities certainly are entitled to restrict access to their library resources, including electronic resources, to faculty members, staff members, students, and other authorized users, such as alumni and recognized scholars from other institutions, in accordance with policies adopted by the institution with the participation of the faculty. But the extent to which access to electronic materials may be limited is not always under the control of the library or even of the institution. Third-party vendors may seek to impose restrictions on access that go beyond those claimed by the institution itself, and such restrictions are rarely defined by faculty governance structures. Those vendors may also impose auditing requirements that are in tension with librarians' obligations to respect the confidentiality of patrons.

Concerns about access were heightened in early 2013 following the tragic suicide of open-access advocate Aaron Swartz. In 2011, a federal grand jury had indicted Swartz for the theft of millions of journal articles through the JSTOR account of the Massachusetts Institute of Technology. It was thought that Swartz had wanted to make all of those articles freely available. Authorities charged him with having used an MIT guest account, even though he did not have a legal right to do so. At the time of his death, Swartz faced millions of dollars in fines and legal costs and decades in prison if convicted. He reportedly had suffered from depression, but there was speculation that his legal troubles led to his suicide.

Although JSTOR declined to pursue action against Swartz, some charged that "MIT refused to stand up for Aaron and its own community's most cherished principles."[5] Ironically, however, it was MIT's relatively open policy of access to its network that enabled Swartz to obtain the downloaded materials. In its own subsequent investigation of the matter, MIT acknowledged that it had missed an opportunity to emerge as a leader in the national discussion on law and the

Internet. But the university denied having had any active role in his prosecution.[6]

Scholars have also debated whether Swartz's action was actually a kind of theft. "The 'property' Aaron had 'stolen,' we were told, was worth 'millions of dollars,' " wrote Harvard law professor Lawrence Lessig, "with the hint, and then the suggestion, that his aim must have been to profit from his crime. But anyone who says that there is money to be made in a stash of academic articles is either an idiot or a liar."[7]

The complicated copyright and other issues raised by the open-access movement are beyond the scope of this report. While the digital world has offered great promise to make information accessible to a global community, commercial forces have locked up most research behind paywalls and ever-more-restrictive licensing agreements. Faculty members who produce research in digital form frequently do not control how that research may be accessed and by whom. The AAUP's *Statement on Copyright* affirmed that "it has been the prevailing academic practice to treat the faculty member as the copyright owner of works that are created independently and at the faculty member's own initiative for traditional academic purposes."[8] Any consideration of open access must start from this principle.[9]

Often college and university libraries are themselves compelled to accede to the demands of outside vendors. Libraries and librarians can, however, promote open access to information by supporting institutional repositories, hosting open-access journals, and working with faculty members to promote the value of more open modes of scholarly communication. Libraries may also collaborate with others or work independently to develop a role as publisher both for new content and through digitization of material that is in the public domain or otherwise lawfully available for digitization.[10]

When resources are provided by third-party vendors, the library may also lose control over privacy and confidentiality. When a faculty member visits the library to read a book or a journal article, this activity takes place without triggering any recordkeeping or permissions issues. In the electronic journal and e-book environment, however, records of access and permissions may be critical to resolving issues concerning licensing and copyright infringement, and the existence of such records may compromise user confidentiality. Sometimes the identity of a person reading a resource is even embedded—both electronically and in text—in the journal article. Such features may violate state laws protecting the confidentiality of library circulation records.

The commitment of libraries and librarians to maximizing access to information and protecting user privacy and confidentiality should not change in the face of new technologies. The maintenance of usage logs for licensing reasons, for diagnosing technical problems, or for monitoring computer performance may be necessary, but libraries must strive to minimize such monitoring and to compile information as much as possible only in the aggregate. So, for example, when the library identifies a user as authorized to gain access to a journal held by another entity, it should indicate that the user is affiliated with the institution without sharing that user's identity.

Nevertheless, third-party vendors may gain access to user information, especially when these vendors offer research tools such as customized portals, saved searches, or e-mail alerts on research topics. How these vendors employ such information and who can gain access to it may be beyond the library's control. Librarians thus have a responsibility to educate users about the potential risks of using third-party tools.

Faculty members can also play a role in shaping the policies of publishers and online vendors regarding access to published research and monitoring of individual users through their roles as members of editorial boards and holders of managerial positions in academic societies and with private publishers. Faculty members in these positions can work with academic libraries to collaborate on cost-effective business models that encourage broad and confidential access to publications.

College and university libraries need to review existing policies on privacy and confidentiality to ensure that they have kept pace with practices and technologies in the library.[11] *In addition, when negotiating contracts with vendors, librarians should require those vendors to protect user information to the same degree as if it were in the custody of a library.* And, building on the success of laws in forty-eight states that protect the confidentiality of library users, as well as provisions of the Family Educational Rights and Privacy Act that protect the privacy of educational records, colleges and universities should advocate additional legislation that would provide the same level of protection to information held by third parties on behalf of libraries and their users, whether it is library-controlled information hosted on a server in another state, cloud-hosted information, or user-supplied information in a vendor's customizable portal.

The 2004 report noted that "in many disciplines, scholars may quite legitimately share material that would be deemed 'sexually explicit'—art, anatomy, psychology, etc. Such sharing is at least as likely to occur electronically as it has traditionally occurred in print. The difference in medium should no more affect the validity of such exchanges than it should justify a double standard elsewhere." AAUP policy elsewhere recognizes that academic freedom includes freedom of artistic expression "in visual and performing arts."[12] Increasingly, artistic expression that challenges conventional tastes and norms involves digital images, even more than images on canvas and film, or dance. It is thus vital to affirm that academic freedom applies to such novel modes of artistic expression as well as to traditional media. Nonetheless, the 2004 report on electronic communications noted that there may "be legitimate institutional interests in restricting the range of persons eligible to receive and gain access to such material—especially to ensure that minors are not targeted."

Although in 1968 the US Supreme Court recognized that material that is not legally obscene but is "harmful to minors" may be regulated, subsequent rulings have severely limited the application of this principle when it might affect access to such material by adults.[13] In this light, *institutional policy should make clear that faculty members in the course of their research have the right to gain access to and circulate electronically all legal materials, no matter how controversial, even if these might be considered "harmful to minors."*

In particular, colleges and universities should refrain from employment of so-called "filtering" software that limits access to allegedly "harmful" or even "controversial" materials. It is questionable whether such filters are appropriate or effective in school and public libraries, but they surely have no place in higher education facilities. Filters are especially insidious because users often cannot know whether they have been denied access to a site or resource.

B. Security versus Access

In recent years many university information-technology (IT) systems have come under sustained cyberattack, often from overseas. While these attacks have sometimes resulted in the theft of personal information, such as employee social security numbers, they also target faculty research materials, including patentable research, some with vast potential value, in areas as disparate as prescription drugs, computer chips, fuel cells, aircraft, and medical devices. Institutions' infrastructure more generally has also been under threat. Some universities have experienced as many as one hundred thousand hacking attempts each day.[14]

The increased threat of hacking has forced many universities to rethink the basic structure of their computer networks. "A university environment is very different from a corporation or a government agency, because of the kind of openness and free flow of information you're trying to promote," said David J. Shaw, the chief information security officer at Purdue University. "The researchers want to collaborate with others, inside and outside the university, and to share their discoveries."[15]

While many corporate sites restrict resources to employees, university systems tend to be more open, and properly so. The most sensitive data can be housed in the equivalent of small vaults that are less accessible and harder to navigate, use sophisticated data encryption, and sometimes are not even connected to the larger campus network, particularly when the work involves dangerous pathogens or research that could turn into weapons systems.

Some universities no longer allow their professors to take laptops owned or leased by the university to certain countries. In some countries the minute one connects to a network, all data will be copied, or a program or virus will be planted on the computer in hopes that it will be transferred to a home network. Many institutions have become stricter about urging faculty members to follow federal rules that prohibit taking some kinds of sensitive data out of the country or have imposed their own tighter restrictions. Still others require that employees returning from abroad have their computers scrubbed by professionals before they may regain access to university servers.

These are genuine concerns, and universities are well advised to devote resources to protecting their electronic-communications networks. However, every effort should also be made to balance the need for security with the fundamental principles of open scholarly communication.

C. Scholarly Communication and Social Media

The advent of social media has raised some new questions about how scholars communicate about their research. For example, professors who present papers at scholarly conferences often use those occasions to try out new ideas and stimulate discussion. While they may be willing, even eager, to share unpolished or preliminary ideas with a closed group of peers, they may be less happy to have those in attendance broadcast these

ideas through social media. Conference papers are often clearly labeled as "not for circulation." At some meetings, however, attendees at sessions have communicated to others electronically—and often instantaneously—through social media, e-mail, or blogs, reports and comments on papers and statements made by other conference presenters and attendees.[16]

Many academic conferences and some individual sessions have associated Twitter hash tags—at times suggested by the conference organizers. As a result, ideas and information that previously would have been controlled by the presenter and limited to a relatively small audience may quickly become accessible globally. Some have worried that reports on social media of conference proceedings might increase the likelihood that others could appropriate a presenter's new and original ideas before that individual has had an opportunity to develop them. While the concern may be speculative and the risk exaggerated, it is clear that new forms of social media and electronic-communications technologies can make research in progress both more accessible and more vulnerable to intellectual property theft. In effect, anyone with an Internet connection can function as a reporter publishing accounts of others' work.

"The debate over live tweeting at conferences is, in many ways, about control and access: who controls conference space, presentation content, or access to knowledge?" wrote one doctoral student. A professor responded with objections to sharing "other people's work without asking." For some the debate is generational. "I see this as a divide between older and newer forms of academic culture," wrote one younger scholar. "On the traditional model, you don't put an idea out there until it's fully formed and perfect."[17]

Of course, scholars have always debated each other's ideas and will continue to do so. However, *faculty members who use social media to discuss research should keep in mind the intellectual property rights of their colleagues as well as their own academic freedom to comment on and debate new ideas.*

II. Freedom of Teaching

According to the 1940 *Statement of Principles*, "teachers are entitled to freedom in the classroom in discussing their subject." But what constitutes a classroom? The 2004 report noted that "the concept of 'classroom' must be broadened" to reflect how instruction increasingly occurs through a "medium that clearly has no physical boundaries" and that "the 'classroom' must indeed encompass all sites where learning occurs."

If anything, the boundaries of the "classroom" have only expanded in the ensuing period. It is now more common than not for even the most traditional face-to-face classes to include material offered through online learning-management systems. And the rapid development and perhaps overhyped promise of totally online education, including the explosive growth of Massive Open Online Courses (MOOCs) frequently offered by for-profit private corporations, suggest that academic freedom in the online classroom is no less critical than it is in the traditional classroom.

This report is not the place to discuss all the myriad issues of academic freedom, shared governance, intellectual property, and institutional finances raised by the spread of online education. It is critical, however, to reiterate that *a classroom is not simply a physical space, but any location, real or virtual, in which instruction occurs and that in classrooms of all types the protections of academic freedom and of the faculty's rights to intellectual property in lectures, syllabi, exams, and similar materials are as applicable as they have been in the physical classroom.*

In August 2013, the administration reassigned the teaching duties of a tenured professor in Michigan after a student anonymously videotaped part of a ninety-minute lecture, a heavily edited two-minute version of which—described by some as an "anti-Republican rant"—was then aired on a conservative Internet site, on Fox News, and on YouTube, where it was viewed more than 150,000 times. In October 2013, a Wisconsin geography professor sent her students an e-mail message explaining that they could not gain access to census data to complete a required assignment because the "Republican/Tea Party–controlled House of Representatives" had shut down the government, thus closing the Census Bureau's website. After a student posted the message on Twitter, it appeared in a local newspaper and in national conservative media, resulting in numerous complaints to the university, which sent an e-mail message to the campus distancing the institution from the comment.[18]

These and similar incidents demonstrate that electronic media can expand the boundaries of the classroom in new and dramatic ways. And while classroom lectures, syllabi, and even an instructor's e-mail messages to students should be considered the intellectual property of the instructor, much of what teachers distribute to students in the classroom or write in e-mail messages may legally be redistributed by students for noncommercial uses under the "fair-use" principle. Moreover, copyright does not cover

expression that is not reduced to "tangible" form, including extemporaneous utterances such as those of the Michigan professor, as it might in the case of a formal lecture, a PowerPoint presentation, or written material like a syllabus.

Surreptitious recording of classroom speech and activity may exert a chilling effect on the academic freedom of both professors and students.[19] Faculty also should be aware that electronic communications with students can easily be recirculated without the permission of either party.

It should be further noted that new teaching technologies and learning-management systems also allow faculty members and students to be monitored in new ways. Online teaching platforms and learning-management systems may permit faculty members to learn whether students in a class did their work and how long they spent on certain assignments. Conversely, however, a college or university administration could use these systems to determine whether faculty members were logging into the service "enough," spending "adequate" time on certain activities, and the like. Such monitoring should not be permitted without the explicit and voluntary permission of the instructor involved.

Some thorny issues also surround the proliferating use of plagiarism-detection software, such as Turnitin. The benefits (and limitations) of such services are often obvious, but many faculty members are unaware that these services keep databases of student papers, and although these papers apparently are not sold individually, the entire database can be and has been sold to third parties. This practice may raise copyright concerns beyond the scope of this report, but as one 2011 study concluded, it also raises "ethical issues because it denies students notice, access, and choice about the treatment of their personal information." That study proposed a "code of ethics" concerning the use of such services that faculty members may find helpful.[20]

While learning-management systems make it possible for faculty members to keep electronic teaching materials separate from scholarly, political, or personal materials often found on faculty websites, many instructors still frequently post course materials on websites alongside other content, some of which may be controversial. Students who encounter material they find disturbing while they are browsing through a faculty member's website in search of course materials may complain to the administration or even to the courts. While all legal material on faculty websites should enjoy the protections of academic freedom, instructors should exercise care when posting material for courses on sites that also include potentially controversial noninstructional materials.

III. Access to Electronic-Communications Technologies

Colleges and universities commonly adopt formal electronic-communications policies, which define access to the institution's electronic-communications network and, through that network, to the Internet. Such policies generally try to balance the need, on the one hand, to protect the university's electronic resources from outside hacking and to safeguard confidential personal and research information and, on the other hand, to provide free access to authorized users. *Although security and liability concerns may result in legitimate constraints being placed on usage, in general no conditions or restrictions should be imposed on access to and use of electronic-communications technologies more stringent than limits that have been found acceptable for the use of traditional campus channels of communication.*

An institution may, for example, acceptably require each faculty user to obtain and enter a password or to change that password periodically. The university also has an interest in protecting its faculty, staff, and students from spam and in limiting how much bandwidth an individual may use to ensure that computing resources are not overburdened or squandered. However, wholesale bans on streaming video may constitute a violation of academic freedom. Some institutions have imposed limitations on access to streaming video and audio in student dormitories, both to prevent illegal downloading of copyrighted material and to avoid overburdening the network. But such efforts should not be extended to faculty members, who may need access to such sites and materials for their teaching or research. Moreover, restrictions that deny use for "personal matters" or limit usage to "official university business" can reduce productivity and are both unnecessary and problematic, as many private businesses have learned.

In an often well-intentioned effort to reduce spam and prevent the monopolization of bandwidth, some university IT offices have proposed policies under which users of institutional electronic-communications resources must seek advance permission to send messages to large groups of recipients. But even if such measures address the problems of spam and limited bandwidth—and it is questionable whether they do—they only create a much larger and more ominous academic freedom problem because they

amount to de facto prior censorship. Similarly, provisions that have been proposed in some instances to bar communications that purportedly "interfere with the mission of the university" or that violate university policies amount to unwarranted censorship of free expression.

Some states have also barred public employees, including faculty members at public colleges and universities, from employing university electronic-communications resources—for example, a university e-mail account—for political campaigning. In such states, public colleges and universities must clearly define what constitutes such activity. While a public employee may reasonably be barred, for instance, from using a university website to run for public office or raise funds for a campaign, policies that discourage or prohibit, either explicitly or through imprecise or ill-defined language, faculty members, staff members, and students from expressing political preferences clearly violate fundamental principles of academic freedom and free expression.

Electronic resources should also be made available equally to all employees, including faculty members, for the purposes of union or other organizing activity. While the National Labor Relations Board has ruled that private employers may bar employees from using employer-owned e-mail accounts for non-work-related communications, if they do permit such activity they may not discriminate against union-related e-mail use nor can they bar the use of social media for discussion of working conditions.[21] Similarly, senate officers and other faculty representatives engaged in institutional governance activities should have free and unfettered access to university-controlled lists of faculty members they represent, and all faculty members should be able to comment electronically on governance issues without restriction or fear of disciplinary action.

In one 2014 incident, a faculty member in Colorado sent an e-mail message protesting proposed layoffs of faculty at his institution that offered a comparison with the 1914 Ludlow Massacre of striking Colorado miners. The university swiftly terminated the professor's access to the institution's e-mail system, charging that the message in question amounted to a violent threat. Although the administration later restored access, the faculty member's ability to distribute messages on listservs remained severely restricted. While institutions clearly have an obligation to protect members of the community from genuine threats of violence, overbroad interpretations of messages as constituting such threats, as was surely the case in this instance, can violate academic freedom, especially if the accused is denied the protections of academic due process before any adverse action has been taken.[22]

The AAUP has upheld the right of faculty members to speak freely about internal college or university affairs as a fundamental principle of academic freedom that applies as much to electronic communications as it does to written and oral ones. This includes the right of faculty members to communicate with one another about their conditions of employment and to organize on their own behalf.

Frequently university policies attempt to delineate user "rights" and "responsibilities," but too often the emphasis of those policies is mainly on the latter. Administrations at some institutions appear to view computer and Internet access as a lower-order faculty perquisite that may be summarily terminated. Such views need to be rejected unequivocally. Access to campus computing facilities, and through them to the Internet, represents a vital component of faculty status for most scholars and teachers, especially as cost-cutting measures have caused libraries to rely more heavily on electronic instead of print journals. While it would be naive to suggest that circumstances might never warrant withdrawal or suspension of digital access, such access may be denied or limited only for the most serious of reasons (for example, creating and unleashing a destructive virus) and only after the filing of formal charges and compliance with rigorous disciplinary procedures that guarantee the protections of academic due process to the accused individual, even where the transgression may not be so grave as to warrant dismissal or suspension.

A university's policies must specify the infractions that might warrant such a sanction, recognizing only conduct that jeopardizes the system and the access of others. The policy should also prescribe the procedures to be followed in such a case. In exigent circumstances, a faculty member's computer access might be summarily and briefly suspended during an investigation of serious charges of abuse or misuse. Any such suspension should, however, be no longer than necessary to conduct the investigation and should be subject to prior internal faculty review.[23]

Indeed, *any restrictions that an institution may need to impose on access and usage must be narrowly defined and clearly and precisely stated in writing*. In addition, institutions should include in their electronic-communications policy a statement similar to that found in the University of California policy: "In general, the University cannot and does not wish to be the arbiter of the

contents of electronic communications. Neither can the University always protect users from receiving electronic messages they might find offensive."[24]

IV. Outsourcing of Information Technology Resources

Many campuses have considered outsourcing the provision of noninstructional IT resources, such as e-mail servers and document storage. Outsourcing to a technology company can provide advantages to institutions, including lower cost and potentially better security, and help an institution focus on its core mission of education instead of on the provision of services.[25] Prior to the cloud outsourcing model, institutions operated in-house technical resources, and the information generated by their use remained within the confines of the institution. In many cloud models, however, it is assumed, sometimes without explicitly stating so, that the outside service provider can analyze how these resources are used for the provider's own benefit. Thus cloud services proceed from a fundamentally different set of assumptions from those that govern the same services that are provided in-house at institutions.

Electronic communications are vulnerable to a variety of threats. They may contain private or confidential information concerning the development of new drugs, classified research, export-controlled research, and advice to clients visiting institutionally operated legal clinics. They may be targets of government surveillance. Institutions also have special duties, including legal and ethical obligations, among others, to protect information about students.

Outsourcing presents several identifiable risks. Outsource providers may be motivated to offer services that they can develop and serve "at scale" and that do not require special protocols. These services may have been designed for businesses, and thus employees and the services themselves may not be tailored to the special context of higher education. In effect, outsourcing may undermine governance, as the provider may effectively set and change policy without consulting campus IT leadership or the faculty.[26]

Several approaches can strengthen an institution's posture on and commitment to academic freedom even in outsourced situations:

1. Institutions should formally involve the faculty in decisions to outsource core electronic-communications technologies.
2. The selection of an outsource provider must take into consideration other factors besides price, including institutional needs, legal and ethical obligations, and the norms and mission of the institution.
3. IT leadership should carefully evaluate the outsource provider's ability to gain access to content and traffic data. It is important to note that even if a provider promises not to circulate usage data to advertisers, that promise does not foreclose the analysis of electronic-communications data for other purposes, including commercial ones.
4. Faculty members should encourage campus IT leadership to collaborate with other institutions in jointly identifying problems and mitigating risks.
5. IT leadership should carefully evaluate the outside provider's uses, processing, and analysis of user content and transactional data. All uses of data should be reviewed by the institution and specifically authorized.
6. IT leadership should follow policy decisions and changes of outsource providers and notify faculty members when these decisions implicate governance issues.
7. IT leadership should consider technical approaches to reduce "vendor lock-in" and, where possible, to mask content and traffic data from these providers.
8. Contracts with outside vendors of electronic-communications services should explicitly reflect and be consistent with both internal institutional policies regarding such communications and applicable federal and state laws.

V. Unwarranted Inference of Speaking for or Representing the Institution

The 1940 *Statement of Principles* cautions that faculty members "should make every effort to indicate that they are not speaking for the institution" when in fact they are not doing so. The meaning of that constraint is clear enough in the print world. One may refer to one's faculty position and institution "for identification purposes only" in ways that create no tenable inference of institutional attribution. In the digital world, however, avoiding an inappropriate or unwarranted inference may be more difficult.

The very nature of the Internet causes attribution to be decontextualized. A statement made by a faculty member on a website or through e-mail or social media may be recirculated broadly, and any disclaimer that the institution bears no responsibility for the statement may be lost. What about statements made on Twitter, which limits communications to a mere 140 characters? It is hardly reasonable to expect a faculty member to indicate on every tweet that she or he is not speaking for the

institution. And Facebook pages are part of a fixed template that does not allow for a banner disclaimer in a readily visible spot on an individual's main page.

In late 2012, a Florida professor posted on his blog a controversial statement expressing skepticism about official accounts concerning the murder of students at Sandy Hook Elementary School in Connecticut that year. The blog included this statement: "All items published herein represent the views of [the professor] and are not representative of or condoned by [the university]." Yet the administration claimed that even by mentioning his affiliation the professor had failed to distinguish adequately his personal views from those of the university and thereby damaged the institution. As a result, he was issued a formal reprimand.[27]

In a letter to the university president, the AAUP staff wrote that the professor "may indeed have posted highly controversial statements on his website; but it is such speech, in particular, that requires the protection of academic freedom. . . . In our time, when the Internet has become an increasingly important vehicle for free intellectual and political discourse around the world, the [university] administration's action, if allowed to stand, sets a precedent that potentially chills the spirited exchange of ideas—however unpopular, offensive, or controversial—that the academic community has a special responsibility to protect."

Institutions may reasonably take steps to avoid inferences of institutional attribution or agreement in ways that print communications might not warrant. Disclaimers may be useful, though their value is often exaggerated. However, the nature of electronic communication itself tends to decontextualize meaning and attribution, and *faculty members cannot be held responsible for always indicating that they are speaking as individuals and not in the name of their institution, especially if doing so will place an undue burden on the faculty member's ability to express views in electronic media.*

VI. Social Media

The 2004 report essentially assumed that electronic communications were either personal (if not wholly private), as with e-mail messages, or public (or open access), as with websites, blogs, or faculty home pages. The growth of social media calls such a distinction into question.

Faculty use of social media is increasing. In one survey of eight thousand faculty members, 70 percent of all those responding reported having visited a social-media site within the previous month for personal use, a rate that rose to 84 percent when those who use social-media sites less frequently than monthly are added. Of greater relevance to the concerns of this report, more than 55 percent said they had made professional use of social media outside the classes they teach on at least a monthly basis, and 41 percent reported having used social media in their teaching.[28]

Social-media sites blur the distinction between private and public communications in new ways. Unlike blogs or websites, which are generally accessible to anyone with Internet access who goes in search of the site, social-media sites offer the appearance of a space that is simultaneously private and public, one that is on a public medium (the Internet) and yet defined by the user through invitation-only entry points, such as Facebook "friend" requests, and a range of user-controlled privacy settings.

The extent of the privacy of such sites, however, is at the least uncertain and limited, because it is dependent not only on the individual's privacy-setting choices and those of the members in the individual's network but also on the service provider's practices of analyzing data posted on the network. Moreover, social-media providers often modify their policies on privacy and access in ways that their users do not always fully comprehend. Faculty members may believe that their Facebook pages are more secure or private than a personal web page, but that is not necessarily true. The seemingly private nature of sites like Facebook, Flickr, or Pinterest can lead individuals to let their guard down more readily, because they may think they are communicating only to handpicked friends and family members, when in fact those friends and family members may be sharing their utterances with other unintended recipients without the individual's knowledge.[29] These sites are not closed portals, despite what their account controls may suggest. Likewise, an acquaintance may post private information about a faculty member's personal life without that faculty member's knowledge (or vice versa), and the viral nature of social-media sites may then make that comment more public than the original poster intended.

There is evidence that such concerns are not unwarranted. One prominent example was the 2010 case of a Pennsylvania professor who was suspended from her faculty position and escorted off campus by police after a student reported to the administration one of her Facebook status updates ("Had a good day today. Didn't want to kill even one student."). The professor alleged that she did not know that anyone other than her

personal Facebook network could gain access to her status updates.

In another example, also from 2010, the administration at a Catholic theological seminary summarily dismissed an assistant professor of church history and languages who was also the library director, reportedly because of a comment he had posted on a former student's Facebook page a month earlier, predicting that "one day the Catholic Church will . . . approve of openly gay priests." In June 2013, an evolutionary psychology professor sparked an uproar after he told his Twitter followers that overweight students are not cut out for PhD programs. The professor quickly deleted the tweet, but he faced considerable criticism, especially after he tried to justify his comment by claiming it was part of a research project. The administration disciplined him for what he had written.[30]

In September 2013, the administration of Johns Hopkins University asked a professor, a prominent authority on Internet security and privacy issues, to remove a blog post, claiming that the post contained a link to classified information and used the logo of the National Security Agency (NSA) without authorization. The post was about NSA privacy debates and encryption engineering. The university has a number of ties with the NSA. The administration withdrew the request after the professor discussed it on Twitter and in the media.[31]

At the University of Kansas, also in September 2013, a journalism professor, responding to a shooting incident at the Washington Navy Yard in Washington, DC, tweeted a comment about gun control that many gun advocates found offensive. He was barraged with hate messages and death threats, and several legislators called for his dismissal. Although the university publicly reaffirmed its commitment to his freedom of speech, he was suspended to "avoid disruption." However, a suspension designed to protect a faculty member from potentially violent responses to a controversial statement can quite easily become a punishment for the content of the statement, which in this instance was clearly protected by both the First Amendment and principles of academic freedom.[32]

Many faculty members have decided that they will simply not join Facebook or similar sites. Others have decided that it would be improper ever to connect with a student on a social network. Most colleges and universities have yet to formulate policies regarding social-media usage by faculty members. At institutions where such policies exist, the focus is frequently on the university's reputation and not on the faculty's academic freedom. So, for instance, the University of South Carolina Upstate's "Social Media Policy and Procedure Guidelines" includes the following: "The purpose of the Social Media Policy is to ensure accuracy, consistency, integrity, and protection of the identity and image of the University of South Carolina Upstate by providing a set of required standards for social-media content from any department, school, facility, organization, entity, or affiliate."[33] It is unclear whether or to what extent this policy applies to individual faculty members.

The incident cited above at Kansas prompted the Kansas Board of Regents in December 2013 to adopt new rules under which faculty members and other employees may be suspended or dismissed for "improper use of social media." The new policy defined social media as "any facility for online publication and commentary" and covered but was "not limited to blogs, wikis, and social networking sites such as Facebook, LinkedIn, Twitter, Flickr, and YouTube." This definition could arguably include any message that appears electronically, including e-mail messages and online periodicals and books. The policy defined "improper use of social media" in extremely broad terms, including communications made "pursuant to . . . official duties" that are "contrary to the best interest of the university," as well as communication that "impairs discipline by superiors or harmony among co-workers, has a detrimental impact on close working relationships for which personal loyalty and confidence are necessary, impedes the performance of the speaker's official duties, interferes with the regular operation of the university, or otherwise adversely affects the university's ability to efficiently provide services."[34]

The AAUP quickly condemned the policy as "a gross violation of the fundamental principles of academic freedom that have been a cornerstone of American higher education for nearly a century. Not only faculty members, but students and members of the general public benefit from the free exchange of information and ideas that are at the heart of the academic enterprise, whether conducted orally, in print, or electronically."[35] In the face of widespread criticism, the board of regents agreed to work with campus leaders to revise the policy, but it was not withdrawn.

This report recommends that each institution work with its faculty to develop policies governing the use of social media. Any such policy must recognize that social media can be used to make extramural utterances and thus their use is subject to Association-supported principles of academic freedom, which encompass extramural utterances.

As Committee A previously noted regarding extramural utterances, "Professors should also have the freedom to address the larger community with regard to any matter of social, political, economic, or other interest, without institutional discipline or restraint, save in response to fundamental violations of professional ethics or statements that suggest disciplinary incompetence."[36]

Obviously, the literal distinction between "extramural" and "intramural" speech—speech outside or inside the university's walls—has little meaning in the world of cyberspace. But the fundamental meaning of extramural speech, as a shorthand for speech in the public sphere and not in one's area of academic expertise, fully applies in the realm of electronic communications, including social media.

VII. FOIA and Electronic Communications

In several recent instances, outside groups or governmental agencies have sought to obtain records of faculty members' electronic communications. In 2011, Virginia's attorney general Ken Cuccinelli demanded that the University of Virginia turn over all e-mail messages and other communications related to and produced by former professor Michael Mann, a prominent scientist of climate change, on the grounds that these were public records. The university successfully resisted the request, characterizing the investigation as "an unprecedented and improper governmental intrusion into ongoing scientific research," and charged Cuccinelli with targeting Mann because the attorney general "disagrees with his academic research regarding climate change."[37] But no sooner had this effort been thwarted, than a private group, the American Tradition Institute (ATI), filed a FOIA request that mirrored the attorney general's subpoena.

The AAUP and the Union of Concerned Scientists (UCS) filed a joint amicus brief in support of UVA and Professor Mann, urging that "in evaluating disclosure under FOIA, the public's right to know must be balanced against the significant risk of chilling academic freedom that FOIA requests may pose." ATI's request, the brief stated, "strikes at the heart of academic freedom and debate." ATI justified its broad intrusion by claiming that its purpose in seeking the records was to "open to public inspection the workings of a government employee, including the methods and means used to prepare scientific papers and reports that have been strongly criticized for technical errors." The AAUP-UCS brief argued, however, that "in the FOIA context, the public's right to information is not absolute and courts can and do employ a balancing test to weigh the interest of the public's right to know against the equally important interests of academic freedom."[38]

Freedom of information laws are generally beneficial: they enhance public knowledge and debate on the workings of government agencies, including public universities. But as the AAUP-UCS amicus brief pointed out, in some situations a balance must be struck between competing interests. Likewise, the Supreme Court recognized as early as 1957 that politically motivated investigations of universities and scholars can have a chilling effect on academic freedom.[39] Allowing fleeting, often casual e-mail exchanges among scholars to be opened to inspection by groups bent on political attack implicates both privacy and academic freedom concerns. As Committee A previously noted in its report *Access to University Records*, "The presumption of confidentiality is strongest with respect to individual privacy rights; the personal notes and files of teachers and scholars; and proposed and ongoing research, where the dangers of external pressures and publicity can be fatal to the necessary climate of academic freedom."[40]

For example, in 2011, the Republican Party of Wisconsin filed a FOIA request with the University of Wisconsin, demanding that the university release e-mail messages from Professor William Cronon, then president of the American Historical Association, who had criticized the Republican governor's "assault on collective bargaining rights." The administration agreed to release some of Professor Cronon's e-mail messages, excluding "private e-mail exchanges among scholars that fall within the orbit of academic freedom and all that is entailed by it." The administration also excluded messages that contained student information and those "that could be considered personal pursuant to Wisconsin Supreme Court case law."

The University of Wisconsin's then-chancellor Carolyn Martin wrote:

> When faculty members use e-mail or any other medium to develop and share their thoughts with one another, they must be able to assume a right to the privacy of those exchanges, barring violations of state law or university policy. Having every exchange of ideas subject to public exposure puts academic freedom in peril and threatens the processes by which knowledge is created. The consequence for our state will be the loss of the most talented and creative faculty who will choose to leave for universities where collegial exchange and the development of ideas can be undertaken without

fear of premature exposure or reprisal for unpopular positions.

Unfortunately, this position has not always been endorsed by other authorities. In June 2012, the *American Independent News Network* sought documents relating to a study by Professor Mark Regnerus of the University of Texas at Austin. The university asserted that the documents were exempt from disclosure under a section of the Texas Education Code, which covers "technological and scientific information" developed by an institution that can be sold, traded, or licensed for a fee. Moreover, it asserted that the records contained information about third parties. The state attorney general's office rejected these claims, however, and in February 2013 the university released the requested records. By April 2013, the *American Independent* was reporting on material that Regnerus had received. A Florida court then ruled that the University of Central Florida also must share the e-mail messages of Professor James Wright, editor of the journal that published Regnerus's study. The court rejected the university's claims that the e-mail communications are not university records.[41]

It is apparent, then, that faculty members at public universities in Texas, Florida, and other states without scholarly exemption from public-records laws should be aware that titles of books they request from the library, peer-review comments they offer and solicit, and tentative ideas they share with colleagues may be matters for public scrutiny under state FOIA laws.[42]

In this light, faculty members should be advised to segregate, as much as possible, personal from professional correspondence and also segregate correspondence that concerns university business from other professional correspondence, such as work for scholarly publications and organizations. Moreover, given the uncertainty surrounding state FOIA laws, faculty members at public colleges and universities should consider the possibility that every e-mail message they send and receive might become public. Lastly, when such requests are made, faculty members should immediately seek the advice and support of their union (if one exists at their institution) or of legal counsel.

VIII. Defamation

Faculty blog posts, although public and open to all, may be targets of libel actions. In 2013, in separate incidents, two university librarians were sued by the Edwin Mellen Press and its founder, who claimed that negative comments about the press the librarians had posted on the Internet constituted libel. In the first case, Mellen sued an associate librarian at McMaster University in Ontario over a post he had written in 2010, when he was a member of the library faculty at Kansas State University, that described Mellen as a "vanity press" with "few, if any, noted scholars serving as series editors," benefiting largely from librarians not returning books sent for approval at "egregiously high prices." The librarian stated, "As a qualified and experienced librarian, I was sharing a professional opinion for consumption by peers."[43] Although Mellen dropped that suit, another suit by its founder continued. Mellen threatened legal action against the interim library dean at the University of Utah, after he criticized Mellen, in part for its action against the McMaster librarian. Mellen's threats prompted the Society for Scholarly Publishing to remove the Utah dean's posts from its blog, *The Scholarly Kitchen*. The Mellen Press's litigious behavior is clearly incompatible with principles of academic freedom.[44]

Because electronic communications are accessible almost instantaneously around the globe, scholars need to be aware that statements they post on blogs or websites or that they communicate by other electronic means may be subject to the laws of other countries. This fact was highlighted in 2013, when a publisher in India announced its intent to sue for libel a librarian at the University of Colorado at Denver, whose popular blog contains a running list of open-access journals and publishers he deems questionable or predatory. On the blog, the librarian accused the Indian publisher of spamming scholars with invitations to publish, quickly accepting their papers, then charging them a publishing fee of nearly $3,000 after a paper was accepted. A letter from the publisher's attorney sought $1 billion in damages and warned that the librarian could be imprisoned for up to three years under India's Information Technology Act.[45]

Such a suit would likely have little chance of success in US courts, but some other countries' libel laws are less stringent, although in India allegations of misuse of the Information Technology Act have led the Indian government to modify its rules to make them stricter. The all-too-common practice of pursuing libel judgments in other countries, most often England or Wales, where there is a presumption that derogatory statements are false, has been dubbed "libel tourism." In response, the US Congress in 2010 unanimously passed the SPEECH Act, which made foreign libel judgments unenforceable in US courts, unless those judgments are consistent with

the First Amendment.[46] However, a judgment unenforceable in the United States might still be enforceable in the country where it was filed and which a scholar may need to visit. Those who not only communicate and publish in other countries but also travel there for research or teaching should be aware of the legal environment governing their expression in those countries.

IX. Privacy of Electronic Communications

Electronic communications have greatly enhanced the ability to teach, to learn, and to inquire. Such technologies have made collaboration over great distances much more efficient and enabled people to work effectively at any hour and in almost any place. At the same time, the structure of electronic-communications technologies can constrain inquiry. Such technologies are designed to document communications and thus amass records of intellectual activities. These records can distort interactions because electronic communications often lack the subtlety of in-person exchanges. They can also be used to investigate individuals in ways that were impossible just a decade ago. *Efforts to protect privacy in electronic communications are an important instrument for ensuring professional autonomy and breathing space for freedom in the classroom and for the freedom to inquire. Although privacy is framed as an individual right, group or associational privacy is also important to academic freedom and to ensuring a culture of trust at an institution.*

When Congress passed legislation to govern the privacy of e-mail and other electronic-communications technologies, these technologies were used primarily by businesses. As a result, some drew the conclusion that the degree of privacy appropriate to digital communications is substantially lower than that expected for traditional media. In the intervening years, however, the use of these technologies has blossomed among businesses and individuals alike.

The nature of a communications medium may take some toll on privacy. An institutional computing network legitimately "backs up" some portion of each day's e-mail traffic. IT staff members in the normal course of events have a technical degree of access to electronic messages that would be unthinkable for personnel in the university mailroom or the campus telephone network. By its very nature, electronic communication incurs certain risks that have no print counterpart—for example, the potential invasion of the system by hackers, despite the institution's best efforts to discourage and even prevent such intrusions. Some of these risks are simply part of the reality of the digital age and a result of our extensive reliance on computer networks for the conduct of academic discourse. At the same time, some privacy risks are the product of business imperatives rather than technical necessities.

Privacy risks are likely to increase as institutions are called on to address more aggressively the security of college and university networks, as researchers increasingly use digital instead of printed resources, and as distance education and electronic-communications technologies are more generally relied on to execute institutional missions.

Faculty members also bear responsibility for protecting privacy in electronic communications. With the proliferation of BYOD policies, sensitive institutional data are sometimes stored on consumer-level devices. Thought must be given to the storage of student and research data on personal and portable devices in case these devices are compromised, lost, or stolen.

The sensitivity of academic communications and the wide range of scholarly purposes for which digital channels are used warrant a markedly higher level of protection. A fully responsive policy would reflect at least these criteria:

1. The policy should recognize the value of privacy as a condition for academic freedom and the benefits that privacy and autonomy bring to the individual, to groups, and to the culture of an institution. The institution should recognize that faculty members have a reasonable expectation of privacy in their electronic communications and traffic data.
2. The policy should clearly state that the university does not examine or disclose the contents of electronic communications and traffic data without the consent of the individual participating in the communication except in rare and clearly defined cases. Calls to examine electronic communications or transactional information should consider the special nature of the academy, weigh whether the examination would have disproportionately chilling effects on other individuals or the institution generally, and contemplate alternative or less invasive approaches to preserve privacy in communications.
3. Employees who operate and support electronic-communications resources regularly monitor transmissions for the purpose of ensuring reliability and security of those resources and services and, in that process, may observe certain transactional information or the contents of electronic communications. Except

in specifically defined instances or where required by law, they should not be permitted to seek out transactional information or contents when those are not germane to system operations and support or to disclose or otherwise use what they have observed.

4. Faculty members should be involved in the setting of institutional policies surrounding the monitoring of and access to content and traffic data in electronic communications. Policies on electronic communications should enumerate narrow circumstances where institutions can gain access to traffic logs and content unrelated to the technical operation of these services. If a need arises to get access to electronic-communications data, a designated university official should document and handle the request, and all parties to the communication should be notified in ample time for them to pursue protective measures—save in the rare case where any such delay would create imminent risk to human safety or university property. Accessed data may not be used or disseminated more widely than the basis for such exceptional action may warrant.
5. As reliance on electronic-communications technologies grows, more faculty online activities will be subject to being logged. Institutions are encouraged to use several strategies encapsulated by the idea of "privacy by design" to reduce the risk to free inquiry and association from this logging. These strategies include creating logs at the aggregate level, where individuals are not identifiable, when possible; carefully controlling access to these logs; removing identifying information from them; and deleting them according to some reasonable retention policy. These strategies must, of course, be balanced to accommodate legitimate security obligations.

Such principles as these, designed as they are to ensure the privacy of electronic communications, will require careful and extensive study by each institution and the tailoring of specific responses consistent not only with institutional needs and values but also with state and local law. At the same time, it must be acknowledged that whatever legal and policy protections may be available, all faculty members should recognize that in practice the privacy of electronic communications cannot always be protected. In addition to the issues raised previously about FOIA laws, faculty members need to recognize that even encrypted messages can be hacked and even the "safest" firewalls can be breached. Moreover, even the most sensitive and private e-mail messages, social-media postings, and texts can be forwarded to countless people instantaneously.

X. The Role of Faculty and Shared Governance

Some faculty members mistakenly believe that institutional IT policies are strictly under the purview of technology offices, which are thought to possess the requisite expertise to address network security, provision of bandwidth, outsourcing, and similar issues. But the interests of faculty members are not always consonant with those of IT offices. The latter may be charged, for example, with conserving resources, while faculty members need broad access to information and ideas.

Some technology offices may be tempted to employ software features "just because they can," without full consideration of their implications for academic freedom and learning. For example, recent learning-management software allows an institution to disable features that invade privacy. But some technology offices may have a cavalier attitude toward privacy or simply desire to offer all the "bells and whistles" available. Electronic communications are too important for the maintenance and protection of academic freedom to be left entirely to such offices. Faculty members must participate, preferably through representative institutions of shared governance, in the formulation and implementation of policies governing electronic-communications technologies.

However, in order for the faculty to play an active and constructive role in the development and execution of such policies, those faculty members who participate in such work need to become more informed about both the technical issues involved and the broader academic-freedom implications of their decisions. This report is designed to facilitate that process.

Specifically, we recommend the following:

1. Policies and practices regarding information technology should be within the purview of a representative faculty committee. Any new policy or major revision of an existing policy should be subject to approval by a broader faculty body such as a faculty senate.
2. The faculty committee may be drawn from the faculty senate or elected as an ad hoc committee by the faculty; its members should not be appointed by the administration.
3. Faculty members participating in the committee should be familiar with and informed about relevant developments in communications technology so that they are able to recognize potential conflicts with principles of academic freedom.

4. The members of the faculty committee should be provided with all relevant contracts and technical materials necessary to make informed decisions about policies governing electronic communications.
5. Whenever policies are proposed or administrative actions taken with respect to information technology that may directly or indirectly implicate academic freedom, faculty members must be consulted.
6. In those institutions with collective bargaining, faculty unions should seek to include in their collective bargaining agreements protections for academic freedom in electronic communications as described in this report.

Notes

1. *Academe* 91 (January–February 2005): 55–59.

2. Robert M. O'Neil, *Academic Freedom in the Wired World* (Cambridge, MA: Harvard University Press, 2008), 179–80.

3. Carl Straumsheim, "Device Explosion," *Inside Higher Ed*, September 5, 2013, http://www.insidehighered.com/news/2013/09/05/wireless-devices-weigh-down-campus-networks.

4. O'Neil, *Academic Freedom in the Wired World*, 181.

5. Scott Jaschik, "Reacting to Aaron Swartz's Suicide," *Inside Higher Ed*, January 14, 2013, http://www.insidehighered.com/news/2013/01/14/academe-reacts-aaron-swartzs-suicide.

6. Colleen Flaherty, "Could Have Done More," *Inside Higher Ed*, July 31, 2013, http://www.insidehighered.com/news/2013/07/31/mit-releases-report-its-role-case-against-internet-activist-aaron-swartz.

7. Lawrence Lessig, "Prosecutor as Bully," *Lessig Blog*, January 12, 2013, http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully.

8. AAUP, *Policy Documents and Reports*, 11th ed. (Baltimore: Johns Hopkins University Press, 2015), 264.

9. As of August 2013, more than 175 universities had endorsed open access. That month, for instance, the University of California Academic Senate adopted an open-access policy that will make research articles freely available to the public through eScholarship, California's open digital repository. The policy applies to all ten of the system's campuses with more than eight thousand tenured and tenure-track faculty members and will affect as many as forty thousand research papers a year. Faculty members can opt out or ask that their work be embargoed for a period of time, as many journal publishers require. In a departure from many other institutions' open-access policies, UC researchers will also be able to make their work available under commercial as well as noncommercial Creative Commons licenses. UC researchers get an estimated 8 percent of all US research money and produce 2 to 3 percent of peer-reviewed scholarly articles published worldwide every year. See "Open Access Gains Major Support in U. of California's Systemwide Move," *Chronicle of Higher Education*, August 5, 2013.

10. One example of such a collaboration may be found at http://www.philosophersimprint.org/, an open-access online resource for philosophy scholarship, the mission of which is "to overcome [the] obstacles to the free electronic dissemination of scholarship."

11. For more on library privacy and confidentiality policies, see http://www.ala.org/offices/oif/statementspols/otherpolicies/rfidguidelines.

12. "Academic Freedom and Artistic Expression," *Policy Documents and Reports*, 40–41.

13. *Ginsberg* v. *New York*, 390 US 629 (1968). In 1997, the Court struck down the Communications Decency Act, and in 2009, it declined to review a decision by the US Court of Appeals for the Third Circuit striking down the Children's Online Protection Act. *Reno* v. *American Civil Liberties Union*, 521 US 844 (1997) and *ACLU* v. *Mukasey*, 534 F.3d 181 (3rd Cir. 2008), cert. denied, 555 US 1137 (2009).

14. Richard Pérez-Peña, "Universities Face a Rising Barrage of Cyberattacks," *New York Times*, July 16, 2013, http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html.

15. Ibid.

16. Steve Kolowich, "The Academic Twitterazzi," *Inside Higher Ed*, October 2, 2012, http://www.insidehighered.com/news/2012/10/02/scholars-debate-etiquette-live-tweeting-academic-conferences.

17. Ibid.

18. Colleen Flaherty, "Not-So-Great Expectations," *Inside Higher Ed*, October 18, 2013, http://www.insidehighered.com/news/2013/10/18/professors-afforded-few-guarantees-privacy-internet-age.

19. The AAUP has been concerned with this issue since its 1915 *Declaration of Principles on Academic Freedom and Academic Tenure*, which stated, "Discussions in the classroom ought not to be supposed to be utterances for the public at large. They are often designed to provoke opposition or arouse debate." In the 1980s, a group called Accuracy in Academia encouraged students to record professors' classroom statements and send them to the organization to be tested for "accuracy." According to a 1985 statement the AAUP issued jointly with twelve other higher education associations, "The classroom is a place of learning where the professor serves as intellectual guide, and all are encouraged to seek and express the truth as they see it. The presence in the classroom of monitors for an outside organization will have a chilling effect on the academic freedom of both students and faculty members. Students may be discouraged from testing their ideas, and professors may hesitate before presenting new or possibly controversial theories that would stimulate robust intellectual discussion."

20. Bastiaan Vanacker, "Returning Students' Right to Access, Choice, and Notice: A Proposed Code of Ethics for Instructors Using Turnitin," *Ethics and Information Technology* 13 (2011): 327–38.

21. The Guard Publishing Company, d/b/a *The Register Guard*, 351 NLRB 1110 (2007), supplemental

decision, 357 NLRB No. 27 (2011); Hispanics United of Buffalo, Inc., 359 NLRB No. 37 (2012).

22. See http://aaupcolorado.org/2014/01/20/colorado-conference-responds-to-csu-pueblo-president-lesley-di-mare-regarding-the-censure-of-professor-tim-mcgettigan/ for more information about the Colorado incident.

23. AAUP-recommended procedures for the imposition of sanctions, whether minor or severe, may be found in Regulation 7 of the "Recommended Institutional Regulations on Academic Freedom and Tenure," *Policy Documents and Reports*, 85.

24. University of California Electronic Communications Policy, http://policy.ucop.edu/doc/7000470/ElectronicCommunications.

25. Outsourcing of instruction through online education offered by outside providers, however, is a quite different matter.

26. The abbreviation IT is used here and subsequently in reference to those university offices and functions variously called "information technology," "instructional technology," or "institutional technology."

27. Scott Jaschik, "Reprimand for a Blog," *Inside Higher Ed*, April 12, 2013, http://www.insidehighered.com/news/2013/04/12/florida-atlantic-reprimands-professor-over-his-blog.

28. The survey was conducted by the Babson Survey Research Group on behalf of Pearson Learning Solutions. See Jeff Seaman and Hester Tinti-Kane, *Social Media for Teaching and Learning* (Boston: Pearson Learning Solutions, 2013), http://www.pearsonlearningsolutions.com/higher-education/social-media-survey.php.

29. Social-media communications may also be used by the social-media site itself for data-mining purposes.

30. Lauren Ingeno, "#Penalty," *Inside Higher Ed*, August 7, 2013, http://www.insidehighered.com/news/2013/08/07/fat-shaming-professor-faces-censure-university.

31. "Hopkins (Briefly) Asks Professor to Remove Blog Post," *Inside Higher Ed*, September 10, 2013, http://www.insidehighered.com/quicktakes/2013/09/10/hopkins-briefly-asks-professor-remove-blog-post.

32. Scott Rothschild and Ben Unglesbee, "Professor Getting Death Threats over NRA Tweet, Colleagues Support His Free-Speech Rights," *Lawrence Journal-World*, September 23, 2013, http://www2.ljworld.com/news/2013/sep/23/firestorm-over-guths-comment-continues-university-/.

33. University of South Carolina Upstate, "Social Media Policy and Procedure Guidelines," https://www.uscupstate.edu/uploadedFiles/Offices/Communications/social/Social%20Media%20Policy%20Approved.pdf.

34. Kansas Board of Regents, "Policy Chapter II C Suspensions," http://www.kansasregents.org/policy_chapter_ii_c_suspensions.

35. AAUP, "AAUP Statement on the Kansas Board of Regents Social Media Policy," http://www.aaup.org/file/KansasStatement.pdf.

36. "Protecting an Independent Faculty Voice: Academic Freedom after *Garcetti v. Ceballos*," *Policy Documents and Reports*, 126–29.

37. For a summary of key events in the Mann case, see http://www.aaup.org/our-programs/legal-program/legal-roundup-2012#iii.

38. Ibid.

39. *Sweezy v. New Hampshire*, 354 US 234, 250 (1957). ("The essentiality of freedom in the community of American universities is almost self-evident. . . . Scholarship cannot flourish in an atmosphere of suspicion and distrust.")

40. *Policy Documents and Reports*, 62.

41. Zachary M. Schrag, "Happy Goldfish Bowl to You, Professor," *Zachary M. Schrag* (blog), November 28, 2013, http://zacharyschrag.com/2013/11/28/happy-goldfish-bowl-to-you-professor/.

42. A recent survey of how state FOIA laws govern requests for material from public universities found that only twenty-five states offer various degrees of exception for academic materials, with the best statutes in Alaska, Pennsylvania, and Georgia. See Ryan C. Fairchild, "Giving Away the Playbook: How North Carolina's Public Records Law Can Be Used to Harass, Intimidate, and Spy," *North Carolina Law Review* 91 (2013): 2117–78. See also the memorandum about state FOIA laws available at http://www.law.gwu.edu/News/2013-2014events/Documents/ATIvUVA/State_FOI_List.pdf.

43. Colleen Flaherty, "Price of a Bad Review," *Inside Higher Ed*, February 8, 2013, http://www.insidehighered.com/news/2013/02/08/academic-press-sues-librarian-raising-issues-academic-freedom.

44. Ry Rivard, "Call In the Lawyers," *Inside Higher Ed*, April 1, 2013, http://www.insidehighered.com/news/2013/04/01/mellen-press-continues-its-legal-maneuvers-against-critics.

45. Jake New, "Publisher Threatens to Sue Blogger for $1-Billion," *Chronicle of Higher Education*, May 15, 2013, https://chronicle.com/article/Publisher-Threatens-to-Sue/139243/.

46. 124 Stat. 2480–84. SPEECH is the acronym for "Securing the Protection of our Enduring and Established Constitutional Heritage."

The California State University
WORKING FOR CALIFORNIA

Responsible Use Policy

CONTACT

WILLIAM PERRY
CHIEF INFORMATION SECURITY OFFICER
THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR
401 GOLDEN SHORE
LONG BEACH, CA 90802-4210

TELEPHONE: (562) 951-4638
EMAIL: WPERRY@CALSTATE.EDU

Table of Contents

Page

Introduction

The California State University (CSU) provides access to information assets for purposes related to its mission and to the responsibilities and necessary activities of its faculty, students and staff. These resources are vital for the fulfillment of the academic, research and business needs of the CSU community. This policy defines user, system administrator and CSU responsibilities with respect to the use of CSU information assets in conjunction with the CSU Information Security Policy.

The CSU regards the principle of academic freedom to be a key factor in ensuring the effective application of this policy and related standards. Academic freedom is at the heart of a university's fundamental mission of discovery and advancement of knowledge and its dissemination to students and the public. The CSU is committed to upholding and preserving the principles of academic freedom: the rights of faculty to teach, conduct research or other scholarship, and publish free of external constraints other than those normally denoted by the scholarly standards of a discipline.

This policy is intended to define, promote, and encourage responsible use of CSU information assets among members of the CSU community. This policy is not intended to prevent, prohibit, or inhibit the sanctioned use of CSU information assets as required to meet the CSU's core mission and campus academic and administrative purposes.

The requirements stated within this policy must not be taken to supersede or conflict with applicable laws, regulations, collective bargaining agreements or other CSU and campus policies.

1.0 Scope

1.1 It is the collective responsibility of all users to ensure the confidentiality, integrity, and availability of information assets owned, leased, or entrusted to the CSU and to use CSU assets in an effective, efficient, ethical, and legal manner.

The CSU RESPONSIBLE USE POLICY shall apply to the following:

a) All campuses.
b) Central and departmentally managed campus information assets.
c) All users employed by campuses or any other person with access to campus information assets.
d) All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
e) Information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

1.2 Auxiliaries, external businesses and organizations that use CSU information assets must comply with the CSU RESPONSIBLE USE POLICY.

1.3 This policy establishes basic responsibilities for all users, the CSU and campuses, and describes expectations for responsible use in the following sections:

Section 3.0	General Principles	This section sets forth basic policy principles. Situations or behaviors not specifically mentioned in sections 5.0 – 7.0 may be addressed through application of these basic principles.

Section 4.0	User - Responsibilities	This section highlights policy specifics related to access, responsible use, network and information system integrity, trademarks and patents, and incidental use.
Section 5.0	CSU and Campus Responsibilities	This section highlights specific requirements for CSU and campus officials.
Section 6.0	Policy Enforcement	This section describes a process for addressing violations of the CSU RESPONSIBLE USE POLICY.

1.4 The development of this policy was expedited by reference to policies from:

a) CSU campuses: Bakersfield, East Bay, Fresno, Humboldt, Long Beach, Monterey Bay, Northridge, San Diego, San Luis Obispo, San Marcos, and Sacramento

b) Other institutions: Concordia College, Montana State University, University of Albany, University of Michigan, and Virginia Tech

2.0 Policy Management

2.1 The CSU RESPONSIBLE USE POLICY shall be updated as necessary to reflect changes in the CSU's academic, administrative, or technical environments, or applicable laws and regulations. The CSU Chief Information Security Officer shall be responsible for overseeing a periodic review of this policy and communicating any changes or additions to appropriate CSU stakeholders.

2.2 The policy may be augmented, but neither supplanted nor diminished, by additional policies and standards adopted by each campus.

2.3 Each campus through consultation with campus officials and key stakeholders must develop policies, standards, and implementation procedures referenced in the CSU RESPONSIBLE USE POLICY.

3.0 General Principles

3.1 The purpose of these principles is to provide a frame of reference for user responsibilities and to promote the ethical, legal, and secure use of CSU resources for the protection of all members of the CSU community.

3.2 Use of CSU information assets shall be consistent with the education, research, and public service mission of the CSU, applicable laws, regulations, and CSU/campus policies. Note: The term "information assets", along with many other important terms and concepts, are defined in the *CSU ICSUAM Policy Glossary*: https://csyou.calstate.edu/ICSUAM/Pages/Policy-Glossary.aspx.

3.3 All users (e.g., faculty, staff, students, third parties) are required to comply with CSU and campus policies and standards related to information security.

3.4 All users (e.g., faculty, staff, students, business partners) are required to help maintain a safe computing environment by notifying appropriate CSU officials of vulnerabilities, risks, and breaches involving CSU information assets.

3.5 It is the policy of the CSU to make information assets and services accessible in order to meet the needs of CSU students, faculty, staff, and the general public. Information regarding the *Accessible Technology Initiative* can be found at: https://csyou.calstate.edu/Projects-Initiatives/ATI/Pages/default.aspx.

3.6 All users, including those with expanded privileges (e.g., system administrators and service providers), shall respect the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers, graphics, and video.

3.7 The CSU respects freedom of expression in electronic communications on its computing and networking systems. Although this electronic speech has broad protections, all University community members are expected to use the information technology facilities considerately with the understanding that the electronic dissemination of information may be available to a broad and diverse audience including those outside the university.

3.8 Other than publicly designated official CSU sites, the CSU does not generally monitor or restrict content residing on CSU systems or transported across its networks; however, the CSU reserves the right to use appropriate means to safeguard its data, preserve network, and information system integrity, and ensure continued delivery of services to users. These activities are not intended to restrict, monitor, or use the content of legitimate academic and organizational communications.

3.9 In the normal course of system and information security maintenance, both preventive and troubleshooting, system administrators and service providers may be required to view files and monitor content on the CSU and campus networks, equipment, or computing resources. These individuals shall maintain the confidentiality and privacy of information unless otherwise required by law or CSU/campus policy.

3.10 The CSU recognizes and acknowledges employee incidental use of its computing and network resources within the guidelines defined in the “Incidental Use” section of this policy, at paragraph 5.5 below.

3.11 All investigations of CSU or campus policy violations, non-compliance with applicable laws and regulations or contractual agreements will be conducted in accordance with appropriate CSU and campus procedures.

4.0 User Responsibilities

This section describes user responsibilities governing access, responsible use, network and information system integrity, and incidental use. These statements are not designed to prevent, prohibit, or inhibit faculty and staff from fulfilling the mission of the CSU. Rather, these statements are designed to support an environment for teaching and learning by ensuring that CSU resources are used appropriately.

4.1 Responsible Use of Informaton Assets

4.1.1 Users are expected to use good judgment and reasonable care in order to protect and preserve the integrity of CSU equipment, its data and software, and its access.

4.1.2 Users must not use or access CSU information assets in a manner that:

a. Conflicts with the CSU mission;

b. Violates applicable laws, regulations, contractual agreements, CSU/campus policies or standards; or

c. Causes damage to or impairs CSU information assets or the productivity of CSU users through intentional, negligent or reckless action.

4.1.3 Users must take reasonable precautions to avoid introducing harmful software, such as viruses, into CSU computing and networking systems.

4.1.4 Unless appropriately authorized, users must not knowingly disable automated update services configured on CSU computers.

4.1.5 Users must take reasonable precautions to ensure that their devices (e.g., computers, tablets, smart phones) are secure before connecting to CSU information assets.

4.1.6 Users must close or secure connections to CSU information assets (e.g. remote desktop, virtual private network connections.) once they have completed CSU-related activities or when the asset is left unattended.

4.1.7 Users must promptly report the loss or theft of any device, which grants physical access to a CSU facility (e.g., keys, access cards or tokens), or electronic access (passwords or other credentials) to CSU resources.

4.1.8 Users who publish or maintain information on CSU information assets are responsible for ensuring that information they post complies with applicable laws, regulations, and CSU/campus policies concerning copyrighted material and fair use of intellectual property.

4.1.9 Software must be used in a way that is consistent with the relevant license agreement. Unauthorized copies of licensed or copyrighted software may not be created or distributed.

4.1.10 Per Section 8314.5 of the California Government Code, it is unlawful for any state employee, or consultant, to knowingly use a state-owned or state-leased computer to access, view, download, or otherwise obtain obscene matter. “Obscene matter” as used in this section has the meaning specified in Section 311 of the California Penal Code. “State owned or state-leased computer” means a computer owned or leased by a state agency, as defined by Section 11000, including the California State University. This prohibition does not apply to accessing, viewing, downloading, or otherwise obtaining obscene matter for use consistent with legitimate law enforcement purposes, to permit a state agency to conduct an administrative investigation, or for legitimate medical, scientific, or academic purposes.

4.1.11 A user who has knowledge (or reasonable suspicion) of a violation of this policy must follow applicable CSU and campus procedures for reporting the violation. A user must not prevent or obstruct another user from reporting a security incident or policy violation.

4.2 Protection from Data Loss

4.2.1 Individuals who access, transmit, store, or delete Level 1 or Level 2 data as defined in the CSU Data Classification Standard[1] must use all reasonable efforts to prevent unauthorized access and disclosure of confidential, private, or sensitive information.

[1] The CSU Data Classification Standard is located at http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf

a. Users must not provide access or transmit Level 1 or Level 2 data to another user without prior approval from the data owner or custodian.

b. Users must not access or transmit unencrypted Level 1 data over a public network.

4.3 Prohibition Against Unathorized Browsing and Monitoring

4.3.1 The CSU supports and protects the concepts of privacy and protects the confidentiality and integrity of personal information maintained in educational, administrative, or medical records. Information stored in CSU information systems may be subject to privacy laws.

4.3.2 Users must not browse, monitor, alter, or access email messages or stored files in another user's account unless specifically authorized by the user. However, such activity may be permitted under the following conditions:

a) The activity is permitted under CSU or campus policy.

b) The activity is defined in the user's job description.

c) The activity is conducted under the authority and supervision of an approved CSU official acting within his or her job responsibilities.

d) The activity is part of a classroom exercise conducted under the supervision of a faculty member. In this case, the faculty member must ensure the exercise does not result in a breach of confidentiality, availability, and integrity of CSU information assets.

e) The activity is conducted to comply with an applicable law, regulation, or under the guidance of law enforcement or legal counsel.

4.4 Responsibillity of Account Owners

4.4.1 The owner or custodian of credentials, such as a username and password, that permit access to a CSU information system or network resource is responsible for all activity initiated by the user and performed under his/her credentials. The user shall assist in the investigation and resolution of a security incident regardless of whether or not the activity occurred without the user's knowledge and as a result of circumstances outside his or her control.

4.4.2 Users must take reasonable steps to appropriately protect their credentials from becoming known by, or used by others.

a. Users who have been authorized to use a password-protected account must follow established procedures for setting, maintaining, and changing passwords. Unless specific prior authorization has been granted, users are prohibited from:

b. Using or attempting to use the account to access, modify, or destroy CSU or non-CSU information assets for which a user is not normally authorized.

c. Disclosing passwords to any party or including passwords in documentation.

d. Embedding passwords in software code.

4.4.3 With the exception of publicly accessible CSU information assets, users must not transfer or provide access to CSU information assets to outside individuals or groups without proper authorization.

4.4.4 Users of CSU information assets must not purposefully misrepresent their identity, either directly or by implication, with the intent of using false identities for inappropriate purposes.

4.4.5 In the few instances where special circumstances or system requirements mandate that multiple users access the same account, extreme care must be used to protect the security of the account and its access password. Management of this account must conform to written or published CSU procedures designed to mitigate risk associated with shared access accounts.

4.5 Incidental Use

4.5.1 University-owned/managed information assets are provided to facilitate a person's essential work as an employee, student, or other role within the University. Use of university owned computer systems for University-related professional development or academic activities such as research or publication is permitted within the limits of system capacities.

4.5.2 Personal use of CSU information assets must be no more than "de minimis" (e.g. must have so little value that accounting for it would be unreasonable or impractical). Individuals may use CSU information assets for occasional incidental and minimal personal use provided such use:

a. Does not violate applicable laws.
b. Is not in pursuit of the individual's private financial gain or advantage
c. Does not interfere with the operation or maintenance of University information assets.
d. Does not interfere with the use of University information assets by others.
e. Does not interfere with the performance of the assigned duties of a university employee.
f. Does not result in a loss to the University.

5.0 CSU Responsibilities

5.1 The CSU has broad responsibilities with respect to protecting its information assets. These include but are not limited to controlling access to information, responding to and addressing information security incidents, complying with laws and regulations, and ensuring the logical and physical security of the underlying technology used to store and transmit information. CSU policies related to these activities are found in the Integrated CSU Administrative Manual and can be accessed at https://csyou.calstate.edu/ICSUAM/Pages/ICSUAM-8000.aspx.

5.2 The CSU retains ownership or stewardship of information assets owned (or managed) by or entrusted to the CSU. The CSU reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across network services; monitoring actions on information systems; checking information systems attached to the network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

6.0 Policy Enforcement

6.1 The CSU respects the rights of its employees and students. In support of the CSU Information Security policies https://csyou.calstate.edu/ICSUAM/Pages/ICSUAM-8000.aspx campuses must establish procedures that ensure investigations involving employees and students suspected of violating the CSU Information Security policy are conducted. These procedures must comply with appropriate laws, regulations, collective bargaining agreements, and CSU/campus policies. Additionally, campuses must develop procedures for reporting violations of this policy.

6.2 The CSU reserves the right to temporarily or permanently suspend, block, or restrict access to information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of CSU resources or to protect the CSU from liability. Suspension, block or restriction to information assets in such a manner as to substantially affect the ability to complete assigned coursework or job duties shall be considered disciplinary actions subject to 7(c)

6.3 Allegations against employees that are sustained may result in disciplinary action. Such actions must be administered in a manner consistent with the terms of the applicable collective bargaining agreement and the California Education code. Student infractions of CSU Information Security policies must be handled in accordance with the established student conduct process. Auxiliary employees who violate the CSU policies may be subject to appropriate disciplinary actions as defined by their organization's policies. Third party service providers who do not comply with CSU policies may be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the CSU.

6.4 The CSU may also refer suspected violations to appropriate law enforcement agencies.