COMPUTING SERVICES
Section: 135-5
Effective: 10/03/2022
Supersedes: 10/22/2009
Review Date: 10/03/2025
Issuance Date: 10/03/2022
Issuing Office: Executive Vice Chancellor Academic Affairs / Vice Chancellor – Chief Financial Officer

UC SAN DIEGO'S ELECTRONIC COMMUNICATIONS PRIVACY AND CONFIDENTIALITY POLICY

Table of Contents

I. INTRODUCTION

The University of California Electronic Communications Policy (the "ECP") was reissued on August 18, 2005. It is posted online at:

http://policy.ucop.edu/doc/7000470/ElectronicCommunications

This policy is the Campus implementation policy of the Privacy and Confidentiality provisions of the ECP, Section IV and related appendices.

This Policy replaces the original policy issued on December 1, 2005, and amended on October 22, 2009, and supersedes previous policies adopted by UC San Diego concerning its subject matter, including PPM 135-5.

II. DEFINITIONS

The capitalized terms used in this Policy are defined below or in the ECP, Appendix A

A. Authorizing Official: The Authorizing Official (whose authority may not be further delegated) is as follows:

1. Vice Chancellor, Student Affairs, is the Authorizing Official for all access without consent requests for electronic communications belonging to students in their capacity as students and to student organizations.
2. Executive Vice Chancellor, Academic Affairs, is the Authorizing Official for all access without consent requests for electronic communications not covered by II.A.1.

If the Authorizing Official specified in this Section faces a conflict of interest, such individual shall recuse themselves and the Chancellor shall act as the Authorizing Official or shall designate another Vice Chancellor to do so.

B. Electronic Communications: Any transfer of signals, writings, images, sounds, data or intelligence that is, created, sent, forwarded, replied to, posted transmitted, distributed,

broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems. For purposes of this Policy, an electronic file that has not been transmitted is not an electronic communication.

C. **Electronic Communications Records:** The contents of electronic communications created, sent, forwarded, replied to, posted, 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, regardless of the ownership of the device or service.

D. **Holder of an Electronic Communications Record or Electronic Communications Holder:** An electronic communications user who, at a given point in time, is in possession 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.

E. **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.

F. **UC San Diego Electronic Communication Services:** Electronic Communications Systems or Services as defined by the ECP that are operated by UC San Diego.

III. PRIVACY OF ELECTRONIC COMMUNICATIONS RECORDS

A. Examination and Disclosure

Examination or disclosure of the contents of an Electronic Communications Record within or using UC San Diego Electronic Communication Services or resources or related to university business shall occur only as provided in this policy.

1. Consent

   The University may examine or disclose Electronic Communications Records with the advance written or oral consent of a Holder of the Electronic Communications Record. Where there are two or more Holders of an Electronic Communications Record, the consent of only one Holder of an Electronic Communications Record is required. When no Holder of an Electronic Communications Record is available to give consent, the procedures in Section III.A.2 of this Policy shall be followed.

2. Without Consent

   a. The University may examine or disclose Electronic Communications Records if authorized in advance and in writing by the Authorizing Official. The grounds for such authorization are specified in the ECP and generally exist in any of the following circumstances:

      i. where required by and consistent with law,
      ii. where there are Compelling Circumstances,
      iii. in the case of time-dependent, critical operational circumstances, or
      iv. when there is substantiated reason to believe that violations of law or University policies specified in ECP Appendix C have taken place

   b. In Emergency Circumstances as defined in the ECP, the University may examine or disclose Electronic Communications Records without Authorizing Official approval. In such cases, the examination or disclosure shall be the least perusal of contents and the least action necessary to resolve the emergency, and ratification of the examination or disclosure shall subsequently be sought without delay from the Authorizing Official.

c. The University's Internal Audit department may examine or disclose Electronic Communications Records in accordance with the UC Internal Audit Charter, except where prohibited by law.

3. Separated and Deceased Users

When a user of UC San Diego Electronic Communication Services dies or separates from UC San Diego, UC San Diego is deemed to be the Holder of that person's Electronic Communications Records. Electronic Communication Records of student employees will be treated as employee records. Access to separated users' records shall be in accordance with this Policy.

UC San Diego maintains the Electronic Communications Records of deceased students for 90 days and the Electronic Communications Records of deceased employees and others as required by the UC Records Management Program. UC San Diego does not release the personal Electronic Communication Records of deceased individuals unless the release is required by law, necessary for an investigation or litigation, there is written consent from the individual prior to death, or pursuant to the Examination without Consent procedures above.

4. System Monitoring and Analytics

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. University employees who operate and support electronic communications resources may provide aggregated or de-identified transactional information to University employees who administer university programs for the purpose of conducting analytics in support of the programs they administer. These processes are not considered an "examination or disclosure" of Electronic Communications Records for purposes of this policy. However, in these processes, employees might observe certain transactional information or the contents of electronic communications.

Except as provided elsewhere in this Policy or by law, these employees are not permitted to seek out transactional information or contents when not germane to system operations and support or required for program support, or to disclose or otherwise use what they have observed, except if they inadvertently discover or suspect improper governmental activity (including violations of law or University policy), reporting of which shall be consistent with the Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (the "Whistleblower Policy"). In the process of such access, 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 personnel from the prohibition against disclosure of personal or confidential information.

B. Documentation

Only university employees with a legitimate business or educational purpose may request access without consent to Electronic Communications Records. All such requesters must submit the following information for an access without consent request:

1. Name and contact information of requester
2. Name and affiliation (*e.g.*, employee or student) of the Holder of the Electronic Communications Record
3. Dates of relevant records sought
4. Whether the Holder of the Electronic Communications Records has been contacted for consent and the result of such request or the reasons why consent was not requested
5. The basis for accessing records, explicitly identifying the circumstances, as required in

III.A.2(a) above, and including the law and/or specific policy identified in ECP Appendix C, if applicable
6. Time frame for notification per III.c. below
7. Description of the account or record requested
8. Explanation of why the specific account or record is relevant and required for the circumstances
9. Names of individuals who will conduct the requested search and access the results
10. Efforts to ensure least perusal of content
11. Description of search protocol (*e.g.*, search terms to be used, where and how search will occur)
12. Anticipated disposition of records once the circumstances permitting access have passed

Requesters are highly encouraged to utilize the Request for Authorization to Access Electronic Records Without Consent (AWOC) form available from the Campus Privacy Office to submit requests. The required documentation must be reviewed by the Campus Privacy Officer and Campus Counsel prior to approval by the Authorizing Official.

Documentation of the approved or denied request shall be kept on file with the Campus Privacy Office.

C. Notification

In all cases of examination or disclosure without consent, the perusal of Electronic Communications Records and the action taken to resolve an emergency or other situation shall be limited to the least perusal and action necessary to resolve the emergency or other situation. In all such cases, the Authorizing Official or designee shall notify the Holder of the Electronic Communications Records whose account was examined of the action(s) taken and the reasons for the action(s) taken at the earliest appropriate opportunity.

D. Report

The Campus Privacy Office shall be responsible for providing the Office of the President with a report summarizing instances of authorized or emergency non-consensual access.

E. Subpoenas, Search Warrants and Discovery

Subpoenas, search warrants, and discovery requests are not subject to Sections III.A.1 and III.A.2. Subpoenas shall be processed in accordance with applicable federal and state laws and University policies, including PPM 470-1 "UCSD Guidelines for Serving, Accepting & Responding to Subpoenas", located online at http://adminrecords.ucsd.edu/ppm/docs/470-1.html Search warrants and discovery requests will be processed as directed by the UC San Diego Office of Campus Counsel.

IV. PRESERVATION OF EVIDENCE

In order to preserve evidence, UC San Diego may copy without notice Electronic Communications Records stored on or transmitted through UC San Diego Electronic Communication Services; provided, however, that Electronic Communications Records copied for this purpose shall not be reviewed by a human being unless (a) consent of a Holder of the Electronic Communications Record is obtained or (b) access without consent is permitted pursuant to this Policy

V. VIOLATIONS OF POLICY - SANCTIONS IN ADDITION TO ACCESS RESTRICTIONS

Violations of this Policy may subject a person to legal penalties and discipline within the University system. Faculty and staff members of the University who violate this policy will be subject to discipline under the Academic Personnel Manual, the Personnel Policies for UC Staff Members, the Bylaws of the Academic Senate, and collective bargaining agreements, as applicable. Students, registered student organizations, and college organizations that violate this policy will be subject to disciplinary sanctions in accordance with the UC San Diego Student Conduct Procedures.

VI. REFERENCES

The following list identifies sources referenced in or used as background for this UC San Diego Communications Procedures and Practices document. Users of this document may also wish to consult the general list of University Policies and Guidelines contained in Appendix B of the ECP.

Academic Personnel Manual (APM): 140 Non-Senate Academic Appointees-Grievances

Business & Finance Bulletin (BFB): IS-3 Electronic Information Security

Bylaws of the San Diego Division of the Academic Senate: 230 Privilege and Tenure

Personnel Policies for UC Staff Members Manual (PPSM): 70 Complaint Resolution

Policy and Procedure Manual (PPM):

160-2	Disclosure of Information from Student Records
480-3	Responsibilities and Guidelines for Handling Records Containing Information About Individuals

University of California Policies Applying to Campus Activities, Organizations, and Students:

100	Policy on Student Conduct and Discipline
110	Policy on Student Grievance Procedures
130	Policies Applying to Disclosure of Information from Student Records

UCSD Policies & Procedures Applying to Student Activities:

160-10	Student Conduct Procedures
160-11	Student Grievances

COMPUTING SERVICES
Section: 135-5 Appendix A
Effective: 10/03/2022
Supersedes: New
Review Date: 10/03/2025
Issuance Date: 10/03/2022
Issuing Office: Executive Vice Chancellor Academic Affairs / Vice Chancellor – Chief Financial Officer

Appendix A: Frequently Asked Questions

1. Are IP addresses, MAC addresses, and device IDs collected through a UC San Diego Electronic Communications Services considered Electronic Communications Records subject to this policy?
   Yes.

2. Are Learning Management System (LMS, *e.g.*, Canvas) or other application records, including logs and metadata, subject to this policy?
   Yes. Communications and transactional information collected through the LMS and other applications are subject to this policy.

3. Who is the Holder of LMS/application records?
   Individuals who have current access to LMS/application records are Holders of that record. For example, while a course is ongoing, the instructor of record and the student are both Holders of the record. When the course is closed, if the student and instructor no longer have access to the course, they are no longer Holders for purposes of this policy.

4. How does a student access their LMS/application transactional information?
   While the course is ongoing, students may access their transactional information by submitting a request to the ITS Service Desk.

5. After a course has closed, how does a student access their LMS/application records or transactional information?
   S*tudents may submit a request for access under the Family Educational Rights and Privacy Act (FERPA) through the Registrar's office.*

6. Who is the Holder of Electronic Communications Records when the initial account holder has separated from UC San Diego?
   The Dean of Undergraduate Education for undergraduate student records; the Dean of Graduate Division for graduate student records; the Deans of the professional schools for professional students; the department or unit head for staff records; and the AVC-Academic Personnel for faculty and researcher records.

7. Are records collected through security cameras, CCTVs, and door access logs Electronic Communications Records for purposes of this policy?
   No.