

---

## UCLA Policy 410: Nonconsensual Access to Electronic Communications Records

---

Issuing Officer: Vice Provost, Information Technology  
Responsible Dept: Office of Information Technology  
Effective Date: August 16, 2010  
Supersedes: New

---

**I. REFERENCES**  
**II. PURPOSE**  
**III. DEFINITIONS**  
**IV. STATEMENT**  
**V. ATTACHMENTS**

### I. REFERENCES

1. University of California Electronic Communications Policy;
2. UCLA Policy 455, UCLA Email Policy and Guidelines;
3. UCLA Procedure 120.1, Producing Records Under Subpoena Duces Tecum and Deposition Subpoenas.

### II. PURPOSE

University employees are expected to comply with University requests for access to Electronic Communications Records in their Possession that pertain to the business of the University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on electronic equipment or devices housed or owned by the University. This Policy implements the relevant provisions of the University of California Electronic Communications Policy (ECP) concerning nonconsensual access to Electronic Communications Records when the consent of the record holder cannot be obtained, and supersedes sections V.E. and F. of UCLA Policy 455, UCLA Email Policy and Guidelines, and the UCLA Request Form for Non-consensual Access to Email.

### III. DEFINITIONS

**Compelling Circumstances** are 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 ECP Appendix C, Policies Relating to Access Without Consent, or significant liability to the University or to members of the University community.

**Electronic Communications** means 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. For purposes of this Policy, an electronic file that has not been transmitted is not an Electronic Communication.

**Electronic Communications Records** are 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** are 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 Systems or Services** are 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.

**Emergency Circumstances** means 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** means a member of the academic community defined as Faculty by Academic Personnel Policy, APP 110-4 (14).

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

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

**Substantiated Reason** means reliable evidence indicating that violation of law or of University policies listed in the ECP 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** means 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.

**UCLA Authorizing Official** is the UCLA administrator identified in the table in Section IV.B. with the authority to approve access to a UCLA Electronic Communications user's Electronic Communications Records without the consent of the user under certain circumstances as set forth in the section.

#### **IV. STATEMENT**

A 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 follows:

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 to believe that violations of law or of University policies listed in the ECP Appendix C, Policies Relating to Access Without Consent have taken place; (iii) when there are Compelling Circumstances; or (iv) under Time-dependent, Critical Operational Circumstances.

When under the circumstances described above the contents of Electronic Communications Records must be examined or disclosed without the Holder's consent, authorization for such access must be obtained in accordance with the following procedures.

**A. Access Request**

The person seeking access to the Electronic Communications Records shall make a request in advance of any access by notifying the department or unit head of the affected Holder. Except as noted under Emergency Circumstances in IV.D., below, a “UCLA Request Form for Nonconsensual Access to Electronic Communications Records” (see Attachment A) must be used and all necessary signatures obtained. Campus Counsel should be consulted as to the appropriate basis for the request.

**B. Request for Authorization**

Except in Emergency Circumstances or except for subpoenas or search warrants (see Section IV.H., below), access without consent must be authorized in advance and in writing by the responsible UCLA Authorizing Official. Such authority may not be further redelegated.

The appropriate responsible UCLA Authorizing Official depends upon the status of the affected Holder:

<b>If Holder's Status Is:</b>	<b>UCLA Authorizing Official</b>	<b>In Consultation With:</b>	<b>Authorizes the following:</b>
Faculty	Vice Chancellor, Academic Personnel	Campus Counsel and Chair, Academic Senate (written advice)	Department/Unit Head or Dean
Student (Not in a capacity as a Staff Employee)	Vice Chancellor, Student Affairs	Campus Counsel	Dean of Students
Staff Employee or Student in the capacity as a Staff Employee (Non-Medical Center, Non-Schools of Medicine & Dentistry)	Administrative Vice Chancellor	Campus Counsel and/or Associate Vice Chancellor, Campus Human Resources	Department/Unit Head or Dean
Staff Employee of the Medical Enterprise (Medical Center or Schools of Medicine & Dentistry) or Student in the capacity as such Staff Employee	Associate Vice Chancellor and CEO, Hospital System	Medical Center Counsel and/or Senior Associate Director, Medical Center Human Resources	Department/Unit Head or Associate Administrator

This authority may also be exercised by the Chancellor or the Executive Vice Chancellor & Provost without regard to the status of the affected Holder.

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

Campus Counsel's advice shall be sought prior to authorization because of changing interpretations by the courts of laws affecting the privacy of Electronic Communications, and because of potential conflicts among different applicable laws. Where the examination or disclosure of Electronic Communications held by Faculty is involved, the advice of the Chair of the Campus Academic Senate shall be sought in writing in advance. All such advice shall be given in a timely manner.

**C. Authorization under Special Circumstances**

Authorization under certain special circumstances is to be provided as follows:

- **Violation of Criminal Law**  
The UCLA Police Chief will request authorization for access to Electronic Communications Records when there is a Substantiated Reason to believe that violations of criminal law have taken place, following the procedure set forth above.
- **Preservation of Evidence**  
A Department/Unit Head or Dean may request authorization to take steps to secure Electronic Communications Records to preserve evidence when there is a Substantiated Reason to believe that violations of law or of University policies have taken place, following the procedure set forth

in Section IV A. and B., above. However, no such evidence may be examined or disclosed without written authorization as specified herein.

In the event of Compelling Circumstances the Emergency Circumstances procedure set forth in IV.D., below will be followed instead.

#### **D. Emergency Circumstances**

In Emergency Circumstances 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 above.

If the action taken is not subsequently authorized, the responsible authority shall seek to have the situation restored as closely as possible to that which existed before action was taken.

#### **E. Notification**

The responsible authority or designee shall at the earliest opportunity that is lawful and consistent with other University policies 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, without revealing personally identifiable data. The UCLA Director, Strategic IT and Privacy Policy shall tabulate this data for the campus and provide the report as required by the ECP. A copy of this annual report will be provided to the Chair of the UCLA Academic Senate.

#### **F. Compliance with Law**

Actions taken under this policy, including access to Electronic Communications Records residing on computers not owned or housed by the University, shall be in full compliance with the law and other applicable University policies, including laws and policies listed in ECP Appendix B, References. Advice of counsel always must be sought prior to any action involving Electronic Communications Records (a) stored on equipment not owned or housed by the University, or (b) whose content is protected under the federal Family Educational Rights and Privacy Act of 1974 (see ECP, Student Information).

#### **G. UCLA Recourse**

UCLA Electronic Communications users who believe that actions taken by employees or agents of the University were in violation of this Policy regarding procedures for review and appeal of actions taken under Section IV A.-F. may file a complaint with the appropriate UCLA Authorizing Official as noted above in Section IV.B. The decision of the UCLA Authorizing Official may be appealed to the Executive Vice Chancellor & Provost, whose decision is final.

#### **H. Search Warrants and Subpoenas**

Search warrants and subpoenas are not subject to sections A.-D. and F.-G., above. Search warrants and subpoenas for Electronic Communications Records shall be referred to Campus Counsel or designated campus officials.

**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 UCLA Procedure 120.1, Producing Records Under Subpoena Duces Tecum and Deposition Subpoenas). 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 UCLA Procedure 120.1.

**V. ATTACHMENTS**

- A. UCLA Request Form for Nonconsensual Access to Electronic Communications Records

**Issuing Officer**

**/s/ James Davis**

---

**Vice Provost, Information Technology**

---

**Questions concerning this policy or procedure should be referred to  
the Responsible Department listed at the top of this document.**

---

# UCLA Request Form for Nonconsensual Access to Electronic Communications Records

For more information, see UCLA Policy 410, Nonconsensual Access to Electronic Communications Records

## A. INFORMATION SOUGHT

Name and department of Electronic Communications Record Holder:

\_\_\_\_\_

Attach a description of the Electronic Communications Records for which access is being requested and a detailed explanation of why nonconsensual access is deemed necessary.

## B. BASIS FOR REQUEST

Type of request (check one):

- Prior authorization  
 Post-access authorization: Emergency Circumstances required immediate access. (Attach explanation.)

ECP provisions under which Records are to be accessed (check all that apply):

- Required by and consistent with law  
 Reasonable belief of violation of law or UC Policy  
 Compelling Circumstances  
 Time-dependent, critical operational circumstances

Reason(s) why Holder's consent cannot be obtained (check all that apply):

- Holder has denied a request to allow access  
 Absence, illness or death precludes requesting Holder's consent  
 Compelling Circumstances preclude requesting the Holder's consent

## C. REQUESTOR NAME, TITLE AND DEPARTMENT/UNIT

\_\_\_\_\_

## D. SIGNATURE OF CAMPUS OFFICIALS

Does the Electronic Communications Holder's department/unit head recommend access?  Yes  No

Signature and Title of Electronic Communications Holder's Department/Unit Head

Date: \_\_\_\_\_

Does Counsel or Human Resources recommend access?  Yes  No

Signature of Counsel or Human Resources – check appropriate box:

Date: \_\_\_\_\_

- Campus Counsel  Assoc Vice Chancellor, Campus Human Resources  
 Medical Center Counsel  Sr Assoc Director, Medical Center Human Resources

If the Holder is a Faculty member, does the Academic Senate Chair recommend access?  Yes  No  
Attach written advice provided by the Academic Senate.  Not Faculty

Is Nonconsensual Access Authorized?  Yes  No

Signature of UCLA Authorizing Official (see Policy 410, IV.) – check appropriate box:

Date: \_\_\_\_\_

- Administrative Vice Chancellor  Chancellor  
 Vice Chancellor, Academic Personnel  Executive Vice Chancellor and Provost  
 Vice Chancellor, Student Affairs  
 Assoc Vice Chancellor/CEO Hospital System

## E. COMPLETED FORM ROUTING

Send a copy of this completed form, *regardless of whether access is authorized*, to the Chief Privacy Officer and Director, Strategic IT Policy, Office of Information Technology, 2333 Murphy, 140501 (90095-1405). **Do not include attachments.**

If access is authorized, this completed form may be presented to the appropriate technical administrator who can provide access to the records requested. Any access authorized shall be limited to the least perusal of contents and the least action necessary to resolve the matter.