UC SANTA BARBARA
POLICY AND PROCEDURE

Implementation of Electronic Communications Policy
Contact: Administrative Services/Privacy Officer
Issued: August 12, 2019
Supersedes: Interim Electronic Communications Implementing Guideline 5612 (2000)
Pages: 14

IMPLEMENTATION OF ELECTRONIC COMMUNICATIONS POLICY (IECP)

The principles of academic freedom, freedom of speech, and privacy of information are central to the University of California Electronic Communications Policy (UC ECP) and the Implementation of the Electronic Communications Policy (IECP). Their intent is to engender an environment encouraging the use of electronic communications and other resources critical to the pursuit of teaching, research, public service, learning, and delivery of services. At the same time, the UC ECP and IECP recognize the University's charge to protect its constituents and meet legal and fiduciary obligations. Thus, the UC ECP and the IECP seek a balance between protection of academic freedom, freedom of speech, and privacy of information, within the context of an increasingly hostile and invasive Internet, while considering ease of use and convenience.

The University of California issued the UC ECP on November 17, 2000.[1] The UC ECP clarifies the applicability of law and University policies relating to electronic communications and governs all electronic communications at UC Santa Barbara. Along with the UC ECP, the University of California issued "Implementing Guidelines."[2] The IECP addresses those guidelines and details the specific manner in which UC Santa Barbara will carry out its responsibilities for electronic communications in accordance with the UC ECP.

The IECP does not repeat or elaborate upon all contents of the UC ECP, though some passages repeat to aid users in application of this policy; users must consult the UC ECP for complete policy information.

I. DEFINITIONS

IECP definitions are located in Appendix A of the UC ECP.

II. SCOPE

The scope of the IECP is the same as that of the UC ECP.

III. POLICY

The IECP:

1. Emphasizes University respect for the privacy of Allowable Users; and

2. Outlines a process that (a) assures the least perusal of content and the least action necessary be taken to resolve issues involving monitoring, inspection, and disclosure

[1] The UC ECP was revised in 2005.
[2] The Implementing Guidelines were revised in 2005 and 2011, respectively.

of Electronic Communications; and (b) assures that an Allowable User is promptly notified of any adverse action taken and of the procedures for recourse.

UC Santa Barbara divisions and departments may implement additional local practice and procedure to refine the UC ECP and IECP to meet their business objectives so long as such additional practice or procedure complies with the UC ECP and IECP. Additional local practice or procedure may not be more permissive than the UC ECP or IECP, though it may be more restrictive. Any division or department that adopts local practice or procedure must provide a written copy of the local practice or procedure to all affected Allowable Users and to the campus privacy officer.

A. Allowable Users

1. UC ECP Section III.C.1 designates University students, faculty, staff, and others affiliated with the University (including those in programs, contract, or license relationships with the University as eligible to use the University Electronic Communications Systems, Services or Resources in accordance with ECP Sections III.D, Allowable Use) as Allowable Users. Use of Electronic Communication Resources by an Allowable User is a privilege, not a right, and is revocable as specified by IECP Section III.E 'Revocation of Allowable User Status and Access Restriction.'

2. Allowable User status generally begins upon affiliation with the University and continues until separation from the University, however, Allowable User status may be terminated upon notice of termination for Allowable Users who have access to critical infrastructure, vital records, or information classified P3 or P4 under IS-3. Under extraordinary circumstances, and where approved by the Associate Vice Chancellor for Information Technology (AVCIT), limited user status may be granted to faculty and staff after termination. Upon statement of intent to register, prospective students gain limited user status to facilitate their interaction with the University. Students retain limited user status until 13 months after they last attend.

B. Notification

1. Faculty and Staff

When new faculty and staff become Allowable Users (i.e. have access to Electronic Communications Services or Resources), the new faculty/staff must receive a copy of the UC ECP and the IECP and/or the web address for the UC ECP and the IECP with sufficient instruction to access them on-line. The department administrator is responsible for providing this access. Additionally,

Department and Unit Administrators, or their designees, must inform their faculty and staff that use of Electronic Communications Services and Resources implies the user:

a. Has read and understands the ECP and IECP; and
b. Acknowledges that usage that does not comply with the UC ECP or IECP may result in sanctions as set forth therein.

Department and Unit Administrators must include this policy requirement in their department's new employee orientation packets/check-off procedures and annotate the date when the new employee receives notice of the ECP and IECP. Department or Unit Administrators, or their designees, must inform their faculty and staff of the department's mail/files backup practices. In order to facilitate this notice requirement, Electronic Communications Service Providers must describe their back-up practices to the departments they serve.

2. Students

Upon signing a contract for Electronic Communications Service, students must receive a copy of the UC ECP and the IECP or the web address and instruction for accessing the UC ECP and IECP on-line and be informed of the service provider's mail/files back-up practices.

Student Communications Service Provider contracts must state: "Use of electronic Communications Services implies acknowledgment that you will use the services consistent with the University Electronic Communications Policy (UC ECP) and Campus Implementing Guidelines (IECP). Use that does not comply with the UC ECP or IECP may result in sanctions as defined within these policies."

Annually thereafter, the Communications Service Provider must notify all existing student Allowable Users that, "Continued use of Electronic Communications Services implies acknowledgment that you will use the services consistent with the University Electronic Communications Policy (UC ECP) and Campus Implementing Guidelines (IECP). Use that does not comply with the UC ECP and IECP may result in sanctions as defined within these policies."

C. Allowable Uses

UC Santa Barbara provides Electronic Communications Resources and Services to its Allowable Users for the purpose of education, teaching, research, and university business. In general, Electronic Communications Resources must be used with the same discretion as all other university resources, carefully assuring that use is a benefit to the University and not for personal benefit or gain. Electronic Communications traveling to[3] or from an Allowable User, or through campus networks, must be for lawful purposes and consistent with state and federal laws and other university policies, including those pertaining to IT Accessibility. Use of Electronic Communications Resources and Services must comply with the Digital Millennium Copyright Act as implemented at UC Santa Barbara.

[3] Allowable Users are not responsible for unsolicited electronic communications in violation of this policy.

1. Personal Use

   Incidental personal use of Electronic Communication Services and Resources is an Allowable Use, but such usage must be consistent with the limitations set forth in the UC ECP Section III.D.8. Use of Electronic Communication Services and Resources for personal gain or in support of any improper governmental activity is not permissible, however.

   Personal Webpages[4] within the University domain must not be posted anonymously and must comply with Section III.C.2 of the IECP, below. Any Personal Webpage that inaccurately gives the impression that the author represents the University must include an explicit disclaimer. An example of acceptable wording for such a disclaimer is, "These statements are my own, not those of the Regents of the University of California."

2. Uses Not Allowed

   a. An Allowable User must not interfere with the normal operation of Electronic Communication Services and Resources. Examples of activities that may interfere include, but are not limited to, mining for electronic currency, posting material that will attract undue attention for activities not associated with the University mission, generating spam messages or traffic intended to interfere with the operation of systems outside of the University.

   b. An Allowable User must not claim to represent the University of California beyond their specific title and job function. Any communication that may be reasonably construed as one coming from the University rather than an individual must be accompanied by the disclaimer, "These statements are my own, not those of the Regents of the University of California." (See, Use of University Name and Acknowledgements and Advertising on University Electronic Resources.)

   c. An Allowable User must not give the impression that they are making an endorsement by the University of California. This disclaimer must accompany any communication that may be reasonably construed as an endorsement on behalf of the University: "References or pointers to non-University entities or resources do not represent endorsement by the Regents of the University of California." (See, Use of University Name and Acknowledgements and Advertising on University Electronic Resources.)

   d. Communications reasonably construed as a conflict of interest with the University are not permissible. A conflict of interest is any outside employment or professional activities, personal financial interests, or acceptance of benefits from third parties that may create actual or perceived

[4] A Personal Webpages is any webpage posted by or on behalf of an individual rather than a University department and that does not represent a function of the University.

conflicts between the University's mission and an individual's private interests. For more information on what constitutes a conflict of interest, and for a listing of University policies relating to conflicts of interest, please see the Systemwide Guidance on Conflict of Interest.

D. Continuity of Access to University Records

Department and Unit Administrators must ensure continued access to University Administrative and Electronic Communications Records consistent with the University Records Management Program and the Records Retention and Disposition Policy.

1. Absences:
   Department and Unit Administrators, or their designees, must implement processes and procedures to ensure proper operation of their activities in the absence of any employee by either (1) asking Allowable Users for consent to access electronic records in their absence or (2) engaging one of the techniques or procedures listed in Appendix 2, Section III.B.5.a. An Allowable User may withhold consent without negative affect; however, the provisions for non-consensual access in the UCECP and the IECP will then apply if access to the electronic records becomes necessary in the Allowable User's absence. To ensure proper permission is obtained, Department and Unit Administrators must use the Campus Request for Consensual Access.

2. Separated Employees
   Prior to separation, employees who have not been granted limited user status (Section III.A.2) must be asked to remove any personal records from all storage sources, including email. To assist with meeting continued business operations and retention requirements, Department and Unit Administrators, or designees, must seek authorization for consensual access in writing prior to separation whenever feasible. An Allowable User may withhold consent without negative effect; however, the provisions for non-consensual access in the UCECP and the IECP will then apply.

3. Death:
   In the event of the death of an Allowable User, the procedures outlined in Section III.F of the IECP, Access Without Consent, shall apply unless the Allowable User previously signed a Consensual Access Form allowing for access in the event of death.

E. Revocation of Allowable User Status and Access Restrictions

1. Revocation of Allowable User Status
   Under Exigent Circumstances, Allowable User status may be revoked. Exigent Circumstances include, but are not limited to the following:

   - Danger to life or property;
   - Sabotage;

- Failure to protect against or participation (knowingly or unknowingly) in the spread of malware, viruses, ransomware, worms, denial-of-service attacks, hacking, data theft, and/or phishing;
- Theft of identities or intellectual property;
- Sexual or other forms of harassment; or
- Illegal or personal commercial or promotional use.

Departments must notify the Chief Information Officer (CIO) at the earliest possible time of any circumstances that may constitute Exigent Circumstances. If the activity appears to be criminal in nature, the CIO must notify the Campus Chief of Police.

Revocation of User Status may either be temporary to remedy an Exigent Circumstance that does not constitute a violation of law or policy (e.g. an Allowable User's email is hacked, an Allowable User clicks on a link to a compromised website that hosts malware, etc.) or for a longer term in the event of a suspected law or policy violation. In either circumstance, revocation of Allowable User Status shall be limited to revocation of access to the minimum number of services required to address the Exigent Circumstance.

The AVCIT, CIO, or Chief Information Security Officer (CISO) may withdraw Allowable User status in accordance with this Section.

i. Temporary Revocation and Reinstatement

Notice
Allowable Users subject to a temporary revocation to address an Exigent Circumstance that does not appear to constitute a violation of law or policy must be notified as early as is practicable of the reason for the revocation and a timeline for reinstatement, excepting when there is a legal restriction on notification.

Reinstatement
The AVCIT, CIO, or CISO must reinstate Allowable User status as soon as the cause of the revocation is remedied.

ii. Revocation Based on Suspected Violation of Law or Policy

Notice
Allowable Users subject to a revocation of Allowable User status due to an Exigent Circumstance caused by a suspected violation of law or policy must be notified as soon as is practicable of the reason for the revocation. Additionally, Campus Counsel, the Executive Vice Chancellor (EVC), the Vice Chancellor for Administrative Services (VCAD), or the Vice Chancellor for Student Affairs (VCSA), as appropriate, must be notified of the revocation.

Reinstatement
Allowable User status revoked due to an Exigent Circumstance caused by a suspected violation of law or policy must be reinstated as soon as the cause of the revocation is remedied unless, in consultation with Campus Counsel, EVC, VCAD, and/or VCSA, it is determined that Compelling Circumstances exist that should prevent such reinstatement.

When Compelling Circumstances exist that prevent immediate reinstatement, the University shall proceed in accordance with the applicable complaint and resolution process (APM, PPSM, Student Code of Conduct, or applicable bargaining unit contract) in order to determine the final resolution of the matter.

Appeal

Any Allowable User whose status has been revoked for longer than 48 hours may appeal the revocation to the EVC, VCAD, or VCSA, as appropriate. The EVC, VCAD, or VCSA, must consult with Campus Counsel and the CIO prior to reinstating any Allowable User status. However, reinstatement may only occur after remediation of the Exigent Circumstance prompting the revocation.

iii. Revocation of a Faculty Member's Allowable User Status Lasting Longer Than 48 Hours

In the event of a revocation based on an alleged violation of law or policy by a faculty member, the Academic Senate must be notified when the revocation remains in effect longer than 48 hours. The Academic Senate, in consultation with the EVC, CIO, and Campus Counsel, may recommend reinstatement of Allowable User status for the faculty member for the duration of the complaint and resolution process. However, reinstatement may only occur after remediation of the Exigent Circumstance prompting the revocation.

2. Email
Electronic Communications Service Providers are responsible for protecting and maintaining the integrity of the email system.

a. Restriction of Email Access
The Email Service Manager must take the necessary actions, including restricting or refusing email services, to prevent, to the extent possible, disruption of email services and damage to Allowable Users. Exigent, Emergency, or Compelling Circumstances are the only circumstances under which the Email Services Manager may restrict access in this manner.

b. Required Notice of Restriction
Consistent with law and other University policies, the Email Services Manager must give the reason for, scope, and length of the restriction to the affected email user at the earliest possible opportunity.

c. Resolution
Email access must be restored as soon as the reason for the restriction is remedied, unless Allowable User status has been revoked pursuant to this IECP.

3. Network Connected Devices
The data network is an indispensable part of daily life at the university. It is a shared resource and the number of devices attached to the network continues to grow significantly year over year. The introduction of the Internet of Things (IoT), smartphones, wearable devices, and inexpensive network-connected devices, place additional requirements on the integrity and availability of the network ensured by the Network Citizenship document. **All devices on the network, whether university-provided or personally owned, must operate in a manner that does not put the network or other devices at risk.**

System owners or administrators must maintain secure configuration of their devices, including maintenance of system updates and configurations, consistent with UC BFB IS-3 and related standards.

a. Restriction of Network Access
Consistent with the Network Citizenship document, the Associate Vice Chancellor for Information Technology (AVCIT) may restrict access to the data network under Emergency or Compelling Circumstances or for failure to adhere to minimum device management requirements. The AVCIT may take the following actions:

i. When a device is determined to be vulnerable to remote exploitation, the AVCIT will notify the network administrator serving the device or the device owner, if known, of the device's vulnerability. If, after a reasonable period not longer than five business days, the device remains vulnerable, the AVCIT may restrict or deny network access to the vulnerable device.

ii. Under Emergency Circumstances, such as an active or imminent attack that could exploit a vulnerable device, the AVCIT may proactively deny network access to a vulnerable device to protect the security and availability of the network and other devices.

iii. The AVCIT may immediately deny network access to devices infected with malware if it is determined the device is causing interference with other devices including attempts to identify, exploit, or interfere with the proper operation of other devices. At the discretion of the CISO, a compromised device may remain connected to the network to facilitate investigation,

when requested by law enforcement or to facilitate removal of information not otherwise available.

b. Required Notice of Restriction
When the AVCIT determines there is a need to restrict access to the data network, the AVCIT must notify the network administrator serving the device or the device owner, if known, of the reason for, scope, and length of the restriction as soon as is practicable.

c. Resolution
Restoration of network access must occur as soon as the reason for the restriction is remedied, unless Allowable User status has been revoked pursuant to this IECP.

d. Appeals to restriction of network access
If a device owner or administrator believes that a device should continue to enjoy network access despite notification of device vulnerability or compromise, the owner or administrator must request continued network access from the Security Operations Center. The CISO will review these requests and grant continued access if one or more of the following conditions apply:

i. Mitigating controls can be applied to guard against exploitation or compromise; OR
ii. There are compelling reasons where mitigating controls cannot be applied, with the understanding that immediate denial of access will occur in the event of device compromise.

F. Access Without Consent

Except as described herein, the University does not routinely inspect, monitor, or disclose the contents of Electronic Communications without the Allowable User's consent. However, subject to the UC ECP and IECP requirements for authorization and notification, the University may inspect, monitor, or disclose Electronic Communications or Resources without the consent of the Allowable User in four situations:

1. Where required by and consistent with law;
2. When there is Substantiated Reason to believe that violation(s) of law or of one or more of the University policies listed in UC ECP Appendix C have taken place;
3. When there are Compelling Circumstances; or
4. Under Time-dependent, Critical Operational Circumstances.[5]

In any of the above, four listed situations, authorization for access without consent must be made consistent with section IV.F, et seq. of this policy, depending on

[5] See Appendix A of the UC ECP at pgs. 18 & 19 for definitions of these four situations.

whether the Allowable User in question is faculty, staff, or student. Access without consent may occur without prior authorization only under Emergency Circumstances or where required pursuant to subpoena, search warrant, or preservation hold.[6] Failure of an Allowable User to respond to a request for access within 24 hours is considered an Emergency Circumstance.

Requests for Non-Consensual Access must be submitted in writing to the Campus Privacy Officer except in Emergency Circumstances or when required by subpoena or search warrant. Where access without consent is made under Emergency Circumstances or when required by subpoena or search warrant, appropriate authorization must then be sought as soon as is practicable in accordance with the authorization and notice procedures described in Section IV.F.1, 2,& 3, below, including submission of a written request to the Campus Privacy Officer for records purposes.

The University may only take the least intrusive action necessary to address the concern when granting access without consent. Where possible, those authorized to access an Allowable User's Electronic Communications or Resources should review metadata only.

The Campus Privacy Officer must keep a record of all approvals of authorized, emergency, or subpoena/search warrant-required non-consensual access. Such records will be kept confidential and in conformance to the records retention schedule. The Campus Privacy Officer will publish an annual report of non-consensual access as required by section III.A.1.4 of Attachment 2: Implementation Guidelines of the UCECP.

For the purposes of the UC ECP and the IECP, automated inspection of Electronic Communications to protect the availability, integrity, and reliability of University Electronic Communications Resources or Services does not constitute non-consensual access (*see,* UC ECP Section III.D.7, Interference; IV.C.2.b, System Monitoring; and V.A., Security; see also, Section V.G.5 of the IECP.) Such actions must be consistent with the principle of least perusal as articulated in the ECP.

1. Accessing Faculty Electronic Communications/Resources Without Consent

    a. Authorization
    The Executive Vice Chancellor must approve, in writing, any non-consensual inspection, monitoring, or disclosure of a faculty member's Electronic Communications or Resources, under conditions 1-4 above. In the event that a conflict of interest prevents the Executive Vice Chancellor from approving a Request for Non-Consensual Access, the Assistant Chancellor for Finance and Resource Management shall review and respond to the request in accordance with this policy.

[6] For more information on the exception for Search Warrants, Subpoenas, and preservation holds, see Section IV.B.6 on page 12 of the UCIEP.

b. Advice
Prior to approving a Request for Non-Consensual Access, the Executive Vice Chancellor shall consult with Campus Counsel and obtain the written advice of the Academic Senate. The Academic Senate shall provide written advice to the Executive Vice Chancellor within four weeks.

c. Notice
The Executive Vice Chancellor shall notify the affected faculty member as soon as is practicable, consistent with law and University policy, of the action(s) taken and the reason(s) for such action(s).

d. Recourse
If a faculty member believes that action(s) taken by employees or agents of the University violate this policy, a faculty member may appeal the decision to inspect, monitor, or disclose Electronic Communications or Resources without consent consistent with the Academic Senate grievance procedures.

2. Accessing Staff Electronic Communications/Resources Without Consent

a. Authorization
The Vice Chancellor for Administrative Services must approve, in writing, any non-consensual inspection, monitoring, or disclosure of a staff member's Electronic Communications or Resources, under conditions 1-4 above. In the event that a conflict of interest prevents the Vice Chancellor for Administrative Services from approving a Request for Non-Consensual Access, the Assistant Chancellor for Finance and Resource Management shall review and respond to the request in accordance with this policy.

b. Advice
The Vice Chancellor for Administrative Services will seek University Counsel's advice prior to approving the written request. Additionally, the Vice Chancellor for Administrative Services shall, as appropriate, seek the recommendation of the Director of Human Resources and/or the Chief of Police.

c. Notice
The Vice Chancellor for Administrative Services, in consultation with Campus Counsel, shall notify the affected staff member as soon as is practicable, consistent with law and University policy, of the action(s) taken and the reason(s) for such action(s).

d. Recourse
If a staff member believes that action(s) taken by employees or agents of the University violate this policy, a staff member may appeal the decision to inspect, monitor, or disclose Electronic Communications or Resources without consent consistent with staff complaint procedures under PPSM-70; represented staff must file a grievance under the terms specified by their collective bargaining agreement.

3. Accessing Student Electronic Communications/Resources Without Consent

   a. Authorization
   The Vice Chancellor for Student Affairs must approve, in writing, any non-consensual inspection, monitoring, or disclosure of a student's Electronic Communications or Resources, under conditions 1-4 above. In the event that a conflict of interest prevents the Vice Chancellor for Student Affairs from approving a Request for Non-Consensual Access, the Assistant Chancellor for Finance and Resource Management shall review and respond to the request in accordance with this policy.

   b. Advice
   The Vice Chancellor for Student Affairs will seek University Counsel's advice prior to approving the written request. Additionally, the Vice Chancellor for Student Affairs shall, as appropriate, seek the recommendation of the Dean of Students and/or the Chief of Police.

   c. Notice
   The Vice Chancellor for Student Affairs, in consultation with Campus Counsel, shall notify the affected student as soon as is practicable, consistent with law and University policy, of the action(s) taken and the reason(s) for such action(s).

   d. Recourse
   If a student believes that action(s) taken by employees or agents of the University violate this policy, a student may appeal the decision to inspect, monitor, or disclose Electronic Communications or Resources without consent consistent with student grievance procedures.

G. Privacy Protections and Limits

1. Personal Image or Statement
   Use of another individual's picture, statement, or likeness must comply with applicable laws and UC Policy as set forth in Use of an Individual's Image or Creative Work.

2. Student Information
   Directory Information may only be published on Campus Electronic Resources consistent with FERPA Guidelines. Students who do not want directory information published on University Resources may "Request to Restrict" their data with the Office of the Registrar.

3. Electronically Gathered Data
   See: UC Santa Barbara Privacy Statement.

4. System Monitoring
   The Associate Vice Chancellor for Information Technology shall ensure that all personnel involved in network security operations have read and understood the

UC ECP (particularly, Section IV.C.2.b) and the IECP. Security operating practices must consider the principle of least privilege when designing security-monitoring processes to ensure least perusal by the fewest persons required ensuring secure operation of the network. Any person operating or supporting Electronic Communications Services and Resources may not disclose the contents of any Electronic Communications they have observed, except as required by law or policy. Automated analysis of logs collected from software systems, databases, networks, and devices is a recommended information security practice and is not subject to the non-consensual access provisions of the UC ECP, Section IV.B.

IV. RESPONSIBILITIES

Allowable Users: Must read, understand, and abide by the UC ECP and the IECP.

Assistant Chancellor for Finance and Resource Management: In the event that the Executive Vice Chancellor, Vice Chancellor for Administrative Services, or Vice Chancellor for Student Affairs must recuse him/herself because of personal or conflicting interests regarding Access Restriction or Access Without Consent, the Assistant Chancellor for Finance and Resource Management shall act as a temporary alternate.

Associate Vice Chancellor for Information Technology: Authorized to revoke Allowable User status in accordance with Section III.E.1 of the IECP. Authorized to restrict network access in accordance with Section III.E.3 of the IECP. Approval authority for requests by faculty and staff to retain limited user status after termination. Ensures that all personnel involved in network security operations have read and understood the UC ECP (particularly, Section IV.C.2.b) and the IECP.

Campus Counsel: Must consult, as applicable, on revocation of allowable user status when based on a suspected violation of law or policy and on all requests for access without consent.

Campus Privacy Officer: Responsible for administration of the UC Electronic Communications Policy and Campus Implementing Guidelines. The Campus Privacy Officer coordinates all requests for non-consensual access.

Chief Information Officer: Responsible for designating an Email Services Manager. Authorized to revoke Allowable User status in accordance with Section III.E.1 of the IECP.

Chief Information Security Officer: Authorized to revoke Allowable User status in accordance with Section III.E.1 of the IECP.

Department or Unit Administrators, or their designees, must notify all Allowable Users of the UC ECP and the IECP in accordance with Section III.B.1 of the IECP. Must ensure continuity of access to University Records consistent with Section II.D. of the IECP.

Electronic Communications Services Providers: Shall document and make available general information about (1) the monitoring practices of systems under their control

consistent with UC ECP Section V.B. and (2) the mail/file back-up practices of the department(s) they serve.

Email Services Manager: Designated by the Chief Information Officer; has administrative responsibility for the electronic communications system and may restrict access to email in accordance with Section III.E.2.

Executive Vice Chancellor: Authorizes action and consults with campus stakeholders pursuant to Sections III "E" and "F," "Revocation of Allowable User Status and Access Restrictions" and "Access Without Consent."

Vice Chancellor, Administrative Services: Authorizes action and consults with campus stakeholders pursuant to Sections III "E" and "F," "Revocation of Allowable User Status and Access Restrictions" and "Access Without Consent."

Vice Chancellor for Student Affairs: Authorizes action and consults with campus stakeholders pursuant to Sections III "E" and "F," "Revocation of Allowable User Status and Access Restrictions" and "Access Without Consent."

V. REFERENCES

UC Electronic Communications Policy, issued November 17, 2000. (Revised 2005)
Academic Senate grievance procedures
Acknowledgements and Advertising on University Electronic Resources
Collective Bargaining Agreements
Conflict of Interest
Digital Millennium Copyright Right as implemented at UC Santa Barbara
FERPA Guidelines
IT Accessibility
Network Citizenship Document revised 2004
PPSM-70
Records Retention and Disposition Policy
Request for Consensual Access Form
Request for Non-Consensual Access
Student Grievance Procedures
UC Santa Barbara Privacy Statement
University Records Management Program
Use of an Individual's Image or Creative Work
Use of University Name
Written Release to Use an Individual's Image or Creative Work

Please direct questions about this policy to Campus Privacy Officer. For general policy questions or comments about this website, please contact privacy@ucsb.edu.