University of California, Riverside

Computing and Communications

Electronic Communications Policy (ECP) Overview and Implementation at UCR

Updated February 2006

Table of Contents:

University of California, Riverside

Computing and Communications

Electronic Communications Policy (ECP) Overview and Implementation at UCR

Updated February 2006

Electronic Communications Policy (ECP) Overview

Please visit http://www.ucop.edu/ucophome/policies/ec/ for the complete text of the policy. Please note that neither the overview nor the implementation guidelines contained in this document are designed to replace or supersede any ECP provisions or mandates. Queries relating to the ECP, UCR's ECP implementation, or any background materials should be addressed to the Associate Vice Chancellor, Computing and Communications or the Director of Computing Support Services, Computing and Communications.

I. Introduction

UCR encourages the use of electronic communications resources and makes them widely available to the university community. Nevertheless, as with all university assets, any single individual's use of campus electronic resources is limited by the constraints required for reliable operations of the systems and services that provide electronic communications.

Importantly, UCR in general cannot (and does not wish to be) the arbiter of the contents of electronic communications. Moreover, the University cannot always protect users from receiving electronic communications they might find undesirable or offensive. *(Page 5 ECP.)*

II. Commitment to Confidentiality

UCR recognizes that core University principles relating to academic freedom and shared governance, freedom of speech, and respect for privacy and confidentiality hold important implications for the management and use of campus electronic communications resources. *(Page 10 ECP.)*

With these core principles in mind, UCR does not examine or disclose electronic communications without the holder's consent. *(Page 10 ECP.)*

Under very limited circumstances, and subject to the requirements for authorization, notification, and other conditions specified under UC policy, UCR may deny access to its electronic communications services (Page 9 ECP) and may inspect, monitor, and/or disclose electronic communications. *(Page 10 ECP.)*

UCR (under UC Policy) prohibits employees and others from seeking out, using, or disclosing personal information in electronic communications without authorization and requires employees to take necessary precautions to protect the confidentiality of personal information encountered in the performance of their duties. *(Page 10 ECP.)*

III. Allowable Uses

Use of UCR electronic communications resources is allowable as long as this use supports the threefold mission of the University or the administrative functions that support the mission, and the guidelines of Non-Competition as outlined in the ECP are followed. Also, users may not use the electronic communications resources for unlawful activities, commercial purposes not under the auspices of UCR, personal financial gain, or any other uses that violate campus policies or guidelines. *(Pages 6-7 ECP)*

As a general guideline, allowable use of electronic communications falls into one of the following broad categories: one, creating web sites and electronic mailing lists; two, sending and receiving e-mail and accessing the Internet; three, making telephone calls; and four, use of electronic resources for the purposes of teaching, conducting research, public service, and/or conducting university business.

As a general rule, electronic communications may not be used for the following: one, any illegal activities, including cyberstalking, digital copyright infringement, disrupting Internet and UCR intranet networks and systems (for example by transmitting viruses, sending spam, or hacking into others' transmissions or files), and tapping telephones; two, any activities that violate University policies, including policies on sexual and other harassment; three, any activities that utilize the University's name and/or seal without appropriate approvals; and four, any activities that utilize UCR electronic communications resources for commercial benefit.

IV. Allowable Users

UCR Users: UCR users include UCR students, faculty, staff, and others affiliated with the campus (including those in program, contract, or license relationships with the University). UCR users, in general, are eligible to use UCR electronic communications resources and services for purposes supporting the university's three-fold mission of teaching, research, and public service.

Public Users: Public users and organizations may only access campus electronic communications resources or services under programs sponsored by the UCR or any of its sub-units, as authorized by the Chancellor (e.g. public patrons of the campus library may access the campus wireless network).

V. Access Restrictions

Access to (and use of) campus electronic communications resources and services is a privilege provided at the discretion of the university.

Access may be restricted under the following circumstances *(Page 9 ECP)*:

A. When there is substantial reason to believe that violations of law (e.g. a DMCA violation) or UCR (or University) policies have taken place.

B. When there are compelling circumstances (as defined in U.C. ECP Appendix A).

C. When time-dependent, critical operational circumstances exist (as defined in U.C. ECP Appendix A).

VI. Access without Consent

UCR only permits the inspection, monitoring, or disclosure of electronic communications records without the consent of the holder of such records when one or more of the following apply AND when appropriate campus approvals have been obtained *(Page 10 ECP)*:

A. When required by and consistent with law.

B. When there is substantiated reason to believe that violations of law or of University policies have taken place.

C. When there are compelling circumstances (as defined in U.C. ECP Appendix A).

D. When time-dependent, critical operational circumstances exist (as defined in U.C. ECP Appendix A).

VII. Privacy Protection

UCR observes all appropriate legal and policy requirements relating to privacy protection (including, but not limited to, FERPA requirements, SB1386 requirements, IS-3 requirements, privacy laws relating to telephone use, etc.).

VIII. Security

UCR makes reasonable efforts to provide secure and reliable electronic communications services. All providers of UCR electronic communications resources (e.g. central, departmental, and unit providers) are required to follow sound professional practices in providing for the security of electronic communications records, data, application programs, and systems based on UCR guidelines and IS-3 policy.

The foundations of secure and reliable electronic communications services are systems that incorporate appropriate authentication, authorization, backup and recovery, physical security, logical security, software control, and managerial control mechanisms (again, per campus guidelines and IS3 policy). *(Page 15 ECP).*

IX. Backups

UCR does not maintain central or distributed electronic archives of all electronic communications sent or received. Electronic communications are routinely backed-up; however, this is only to assure system integrity and reliability. Electronic communications backups are not designed to provide for future information retrieval, although back-ups may at times serve the latter purpose incidentally. Providers of University electronic communications services are not required by this university policy to routinely retrieve electronic communications from such back-up facilities for individuals.

X. Responsibilities

UCR Chancellor has appointed the Associate Vice Chancellor, Computing and Communications as the designated coordinator to administer UCR's ECP implementation. In consultation with faculty, staff and students, the AVC Computing and Communication has developed this Electronic Communications Policy Overview and Implementation at UCR.

University of California, Riverside

Computing and Communications

Electronic Communications Policy (ECP) Overview and Implementation at UCR

Updated February 2006

Electronic Communications Policy (ECP) Implementation at UCR

I. Electronic Communication Services.

UCR encourages the use of electronic communications in support of the University's three-fold mission of research, teaching, and public service. UCR allocates its electronic resources with the objective of providing the greatest possible benefit to the entire campus community.

A. Understanding Identity Management at UCR and Access to Electronic Communications Services.

In general, authenticated access to UCR's electronic communications resources is provided via UCR's Identity Management systems and processes. These systems and processes are managed by UCR's central information technology organization, Computing and Communications (C&C). A primary objective of C&C's Identity Management systems and processes is to provide access to electronic communications in a quick, efficient, and secure fashion.

Via UCR's Identity Management processes, campus students, staff, and faculty are provided a common identifier known as a UCR NetID that is used to authenticate individuals to various UCR systems providing electronic communications services.

Highlights of UCR's Identity Management systems and processes include the following:

1. SIS* (for students) and PPS* (for faculty and staff) provide input to the campus Enterprise Directory (UCR utilizes an industry standard directory services and protocols).

* SIS = Student Information System
PPS = Payroll Personnel System

2. Before PPS information is used to populate the Enterprise Directory, departmental administrative staff provides additional information (e.g. working title, secondary titles, etc.) to ensure information contained in the campus Enterprise Directory is as meaningful and robust as possible.

3. Once UCR staff, faculty, and student information makes its way to the Enterprise Directory, individuals are automatically granted access to several electronic communications services (e.g. e-mail, etc.) and are eligible for access to other systems (e.g. electronic travel system).

4. When students are no longer enrolled at UCR, or when employees are terminated and removed from PPS, they are AUTOMATICALLY removed from UCR's Enterprise Directory and access to authenticated electronic communications resources ends.

B. General Notes Relating to Various Electronic Communications Services

Email

UCR email addresses using ucr.edu, provided to employees, students, and affiliates, are considered public records under the California Public Records Act and may be published unless access is restricted under applicable law (e.g. Federal Family Educational Rights and Privacy Act of 1974).

Generic business email addresses (not based on an individual's name) should be used for activities that generate a high volume of departmental or unit e-mail. Such usage that prevents business disruption should reflect departmental personnel change. Examples: cnas@ucr.edu, biochem@ucr.edu, finaid@ucr.edu, parking@ucr.edu, etc. These business designations must be approved by a responsible departmental or unit official and submitted to Computing and Communications for authorization.

Web and Other Services

UCR provides access to web resources in the support of University business.

UCR does not routinely collect information about an individual's web use or sites visited. Except when tracking a reported crime, the monitoring of web sites visited, or web use in general, is not permitted under U.C. policy.

If a campus system automatically collects visitor / user information when an individual visits a UCR web site, notice to that effect should be posted at the beginning of the session and should indicate what information will be collected and how it will be used. Web site visitors / users should be allowed to terminate the session at that point without leaving data behind.

Telephones

In compliance with federal law, the University does not allow audio or video telephone conversations to be recorded or monitored without advising the participants, unless a court has explicitly approved such monitoring or recording and University policy is followed in the conduct of the monitoring or recording. Emergency services shall record 911-type emergency calls in accordance with federal and state laws and regulations.

Radios

Users of telecommunications radio frequency transmitters and receivers will operate in compliance with regulations of the Federal Communications Commission and appropriate University policy.

II. Allowable Users

A. Faculty, Staff and Students

All UCR faculty and staff are allowable electronic communications resource users.

All UCR enrolled students are allowable electronic communications resource users. In some circumstances and for some campus systems, certain non-enrolled individuals (e.g. students who have graduated, prospective students, etc.) are considered allowable electronic communications resource users. Please refer to UCR's Student ECP Guide at http://www.cnc.ucr.edu/studentguide/index.php?content=studentecp

Please see the Identity Management section of this document for additional information.

B. Affiliate

An affiliate is a person who is engaging in official campus business but does not have an entry in PPS (the campus payroll system). This individual may be a consultant on contract, an auditor, or any other identified individual who, for the benefit of the university, should have access to authenticated electronic communications. A responsible department official must approve affiliates in writing, and C&C will subsequently enable their access to electronic communications systems.

C. Public Users

Public users and organizations may only access campus electronic communications resources or services under programs sponsored by the UCR or any of its sub-units as authorized by the Chancellor (e.g. public patrons of the campus library may access the campus wireless network).

PLEASE NOTE: Usage of many UCR electronic resources is governed by license agreements with private vendors that exist to support campus research, teaching, and public service. In general, authorized users of this licensed content include current UCR faculty, students, and staff and on-site public users of UCR electronic resources. Systematic downloading of this licensed content, sharing of data with individuals at other institutions, making content available on openly accessible servers / web sites, and using such articles or information for commercial purposes are, in general, expressly prohibited by university practice and by vendor license agreements.

Misuse of licensed electronic content could result in termination of the license and loss of the use of this material by the entire UCR community. In addition, users should be aware that publishers may monitor use of electronic resources to ensure that the terms of their license agreements are enforced.

D. User Privacy of and Access to Electronic Information

The University respects the privacy of electronic communications users as a core operating principle. Managers of computing systems providing electronic communications services will not inspect, monitor, or disclose the content of electronic mail without the holder's consent except under specific circumstances as defined in the "Access without Consent" section of this document.

III. Allowable Use

As a general guideline, allowable use of electronic communications include falls into one of the following broad categories: one, creating web sites and electronic mailing lists; two, sending and receiving e-mail and accessing the Internet; three, making telephone calls; and four, use of electronic resources for the purposes of teaching, conducting research, public service, and/or conducting university business.

As a general rule, electronic communications may not be used for the following: one, any illegal activities, including cyberstalking, digital copyright infringement, disrupting Internet and UCR intranet networks and systems (for example by transmitting viruses, sending spam, or hacking into others' transmissions or files), and tapping telephones; two, any activities that violate University policies, including policies on sexual and other harassment; three, any activities that utilize the University's name and/or seal without appropriate approvals; and four, any activities that utilize UCR electronic communications resources for commercial benefit.

The following general guidelines should be utilized to determine if a particular application or use of a campus electronic communications resource is allowable:

A. **Purpose** Electronic communications resources may be utilized by university departments, units, or sub-units in support of teaching, research, and public service as well as any administrative functions that support this mission.

B. **Non-Competition** UCR electronic communications resources shall not be provided to consumers or organizations outside the university except by approval of the Chancellor (or the Chancellor's designee). Such services shall support the mission of the university and not be in competition with commercial providers.

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

- unlawful activities;
- commercial purposes not under the auspices of the university;
- personal financial gain;
- 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).

D. **Representation** Users of electronic communications resources must abide by appropriate statutes as well as UC and campus policies on the use of the University's name, seals, and trademarks. Users of electronic communications resources shall not give the impression that they are representing or otherwise making statements on behalf of UCR or any department, unit, or sub-unit of the university unless appropriately authorized to do so.

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

F. False Identity and Anonymity Users of University electronic communications resources shall not, either directly or by implication, employ a *false identity* (e.g. utilize the name or electronic identification of another).

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.

G. Interference University electronic communications resources shall not be used in a manner that could reasonably be expected to cause excessive strain on any campus electronic communications resource or unwarranted or unsolicited interference with others' use of electronic communications resources (examples include sending "spam," engaging in "denial of service attacks", etc.).

H. Personal Use University users of electronic communications resources may use these resources for incidental personal purposes provided that such use does not: one, directly or indirectly interfere with campus electronic communications operations; two, interfere with the user's employment or other obligations to the university; or three, burden UCR 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.

I. Accessibility All electronic communications resources intended to accomplish the academic and administrative tasks of the university shall be accessible to allowable users with disabilities in compliance with law and UC policies.

J. Intellectual Property The use of all campus electronic communications resources must conform to laws and UC policies regarding protection of intellectual property, including laws and policies regarding copyright, patents, and trademarks.

IV. Access Restrictions

Access to (and use of) campus electronic communications resources and services is a privilege provided at the discretion of the university.

Access may be restricted under the following circumstances:

A. When there is substantial reason to believe that violations of law (e.g. a DMCA violation) or UCR (or University) policies have taken place.

B. When there are compelling circumstances (as defined in U.C. policy).

C. When time-dependent, critical operational circumstances exist (as defined in U.C. policy, e.g. denial of services network attack)

Special note relating to access restrictions:

UCR's central information technology organization, Computing and Communication (C&C), employs network and security personnel who have the authority to evaluate the seriousness and immediacy of threats to UCR's information system resources and/or threats emanating from UCR to the Internet at large. Based on the seriousness, immediacy, and potential cost to the university, C&C will take responsible and prudent actions to terminate the threat, therefore balancing the risk the threat poses to both UCR or the Internet as well as the potential negative effects restricting access will have to UCR's research, teaching, and public service mission (for example, balancing issues relating to shutting down network access from a research lab containing a computer that is attacking the Internet). Examples of serious threats include the following:

A. Excessive bandwidth use, enough to cause network performance degradation.

B. Continued off-campus complaints with no response from on-campus responsible parties.

C. Verified open proxy or open mail servers.

D. Attacks observed by C&C's network monitoring systems.

E. Verified DMCA violations.

Please note: Actions to restrict will be governed by definitions for urgency, immediacy, etc. found in UC's Electronic Communications Policy and IS-3. Additionally, in the event that network traffic is inspected to confirm malicious or unauthorized activity, such activity shall be limited to the least perusal of content required to resolve the situation. User consent is not required for these routine monitoring practices

V. Access without Consent

A. *Authorization.* In order to access electronic content without a user's consent, a request must be submitted the Associate Vice Chancellor, Computing & Communications containing a reasonable explanation why such access is required. This request will be evaluated and the situation assessed per UC policy and campus guidelines. If warranted and appropriate, the AVC C&C will forward the request to an authorizing official for approval. Search warrants and subpoenas are not subject to approval by the Authorizing Officials; however search warrants and subpoenas are to be referred to the Associate Vice Chancellor, Computing and Communications. In all circumstances, reasonable attempts must be made to identify alternative means of accessing electronic communications prior to granting nonconsentual access to personal electronic information.

B. *Authorizing Officials:*

Except in emergency circumstances, or for subpoenas or search warrants, access without consent must be authorized in advances as indicated below;

Faculty and Librarian records - Executive Vice Chancellor

Staff and Affiliates – Vice Chancellor of Administration

Students – Vice Chancellor of Student Affairs

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

C. Reasons for Granting Access without Consent:

Access without consent shall be permitted under the following circumstances:

- when required and consistent with law;
- when there is a substantiated reason such as: reliable evidence indicating a violation of law or UC polices (as distinguished from rumor, gossip, or other unreliable evidence);
- when there are compelling circumstances for which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence relating to violations of law or UC policies, or significant liability to the UCR or to members of the university community;
- when there are time-dependent, critical operational circumstances and when failure to act could seriously hamper the university's ability to function administratively or to meets its teaching or research obligations.

D. Notification:

In the event of access without consent, UCR's AVC, Computing and Communications will notify the affected individual of the action(s) taken at the earliest opportunity that is lawful and consistent with other University policy.

Please note: Access without consent will be guided by definitions for compelling circumstances, critical operational circumstances, etc. found in UC's Electronic Communications Policy.

VI. Notes on Privacy

Privacy of and Access to E-mail Content

UCR recognizes that core University principles relating to academic freedom and shared governance, freedom of speech, and respect for privacy and confidentiality hold important implications for the management and use of electronic communications.

With these core principles in mind, UCR does not routinely inspect, monitor, or disclose electronic communications without the holder's consent. Nevertheless, employees who operate and support electronic communications resources regularly monitor transmissions for the purpose of ensuring reliability and security of our resources and services. If in that process an employee observes content or transactional information they are not permitted to disclose or otherwise use what they have observed, unless provided for by this policy.

Systems personnel shall not intentionally search the contents of electronic communications or transactional information except as provided by this policy. However, if in the course of their duties systems personnel

inadvertently discover or suspect improper governmental activities, reporting of such violations shall be consistent with the Whistleblower Policy.

Access by the Public

The California Public Records Act requires UCR to disclose various public records. In response to requests for such disclosure, it may be necessary to access electronic communications records that users consider to be personal to determine whether they are public records that are subject to disclosure. Such requests will be presented to Authorizing Officials as noted in this document. Managers of systems who receive off-campus requests for disclosure of information should forward and coordinate such requests with the Associate Vice Chancellor of Computing and Communications.

Sharing Contents of Electronic Communications Resources

In general, electronic communications resources are no longer considered private if either the sender or recipient voluntarily shares the content with a campus official or a manager of the computing system providing the electronic communication service in question. This sharing of electronic content may occur if an individual is the recipient of unwanted or harassing messages or if the individual encounters a technical problem sending or receiving e-mail. In such cases, campus staff will exercise discretion and professional judgment in sharing the content of the message(s). Appropriate officials with whom electronic content may be shared include, but are not limited to, Human Resources Consultants and/or the Manager of Consulting and Labor Relations, the Academic Personnel Director, the Ombudsman, UCR's various Vice Provosts, Internal Audit, Equal Opportunity /Diversity, and the UCR Police.

Maintenance Needs

Information in e-mail "headers" such as sender, recipient, date and subject may be examined by staff in response to normal operational concerns (e.g. problems with the delivery of email, excessive copies of messages, or excessive length of messages). Certain technical tools used in the management of computer systems may display the entire content of an email (file). In such cases, staff will exercise professional judgment concerning viewing the file's contents.

VII. Terminations and Temporary Absences

Transfer or Termination of E-mail Service

All UCR domain name addresses are the property of UCR. In general, users' access to electronic communication services (and in general, protections afforded users under the UC's Electronic Communications Policy) will be terminated as outlined in the table below.

Situation	Faculty	Staff	Students	Affiliate
Separation of Employment	Visiting Post-Doc 30 days Non-Academic Senate 30 days Academic Senate 90 days	30 days	N/A	N/A
Retiree	Lifetime E-Mail	30 days	N/A	N/A

Degree Award	N/A	N/A	Three Academic Quarters	N/A
Separation of Affiliation	N/A	N/A	N/A	Immediate
Involuntary Termination from University Employment	N/A	Immediate	N/A	N/A

Faculty, staff, and students using departmental or unit e-mail accounts (not C&C accounts) are subject to departmental and unit guidelines for use of these systems, providing such guidelines do not conflict with University policy.

Transferring E-mail Addresses

When an employee transfers from one UCR department to another, the UCRnetID and UCRnetID@ucr.edu email address transfers with the employee. For this reason UCR managers and other responsible departmental officials are encouraged to utilize generic email addresses for critical business functions.

Temporary Absences and Separations

Written approval to access an individual's e-mail (and other electronic information such as documents contained on a personal computer) should be obtained prior to an employee taking a temporary leave (e.g. vacation). If written approval to access electronic content is not obtained prior to the temporary absence, university representatives may not read the e-mail records or access other electronic content.

If an employee is on temporary leave (e.g., vacation, leave of absence, etc.) and access to e-mail or other electronic content is required to sustain university operations, and the employee did not provide permission to access this data prior to beginning the temporary leave, the guidelines for non-consensual access contained in this document must be followed.

VIII. Special note on DMCA

The distribution of copyrighted materials without permission (over the internet) can be a violation of federal law. The law is known as the Digital Millennium Copyright Act of 1998 ("DMCA"). Much of the music, video, or games that are downloaded via programs like KaZaa or eDonkey2000 are distributed without the permission of the copyright owner, and thus these downloads are illegal.

UCR students, staff, and faculty should be aware that colleges and universities must QUICKLY respond to DMCA related inquiries since ISPs (Internet Service Providers, like UCR) can be held liable for copyright infringement if they do not promptly resolve illegal distribution activities once they become aware of them. *As a result, UCR attempts to resolve DMCA queries in the most expeditious manner possible as soon as the campus is informed of a violation.*

Additional information concerning the DMCA and campus procedures and programs relating to the DMCA can be found at dmca.ucr.edu.

IX. Special note on SB1386

Senate Bill 1386 and Assembly Bill 700, effective July 1, 2003, added a new provision to the California Information Practices Act - Civil Code 1798.29, 1798.82. This new provision requires any state agency (including the University of California) with computerized data containing personal information to disclose any breach of security of a system containing such data to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This notice of a security breach must be provided to affected persons in the *most expedient time possible and without unreasonable delay*.

Additional information concerning SB1386 and campus procedures and programs relating to its implementation can be found at cnc.ucr.edu/sb1386.

X. Backups and logs

In order to provide a robust method of recovering from disasters, C&C performs nightly backups of campus electronic communications systems, including UCR's central e-mail servers. The e-mail backups are based on a "single image" of the e-mail system and are not conducive to recovering individual files. UCR's backups are archived on local and remote systems with limited access.

Importantly, UCR does not maintain central or distributed electronic archives of all electronic communications sent or received. The aforementioned backups are designed only to assure system integrity and reliability and are not intended to provide for future information retrieval, although back-ups may at times serve the latter purpose incidentally. Providers of UCR electronic communications services are not required by UC policy to routinely retrieve electronic communications from such back-up facilities for individuals.

Log files from central electronic communications systems are maintained per standard industry practices. E-mail logs, including records of delivery date, recipients, and message IDs, are retained for approximately one week. These logs are kept on secure machines with limited access and are not accessed (normally) by administrators. They are processed automatically (without human intervention) to provide usage statistics and graphs.

XI. Reporting to UCOP

Reports of non-consensual access to UCR electronic communications resources will be reported annually by the Associate Vice Chancellor, Computing and Communication to the Office of Information Resources and Communications (at UCOP) as required by UC policy.

XII. References

1. *National and State Resources*

    A. California Information Practices Act of 1977 (IPA)

(http://www.privacy.ca.gov/code/ipa.htm)

B. California Public Records Act (CPRA) (http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6250-6270)

C. Federal Family Educational Rights and Privacy Act of 1974 (FERPA) (http://www.ucop.edu/ucophome/policies/bfb/rmp8.html#IV

D. State of California Penal Code, Section 502 and 1523 et seq.

2. *University of California Resources*

A. UCOP Electronic Communications Policy, August, 2005 (http://www.ucop.edu/ucophome/policies/ec/)

B. UCOP Policies Applying to Campus Activities, Organizations, and Students, August 1994 (http://www.ucop.edu/ucophome/uwnews/aospol/toc.html)

C. UC Business and Finance Bulletins (http://www.ucop.edu/ucophome/policies/bfb/is3toc.html)

D. UCOP IS-3, Electronic Information Security (http://www.ucop.edu/ucophome/policies/bfb/is3toc.html)

E. UCOP IS-10, Systems Development and Maintenance Standards (http://www.ucop.edu/ucophome/policies/bfb/is10.pdf)

F. UCOP RMP-8, Legal Requirements on Privacy of and Access to Information (http://www.ucop.edu/ucophome/policies/bfb/rmp8toc.html)

G. UCOP Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (the "Whistleblower Policy")

3. *University of California, Riverside Resources*

A. Campus Policies and Procedure Manual http:www.vca.ucr.edu/index.php?content=http://138.23.50.157/policies.html