University of California, Riverside

Computing and Communications

Electronic Communications Policy (ECP) Overview and Implementation at UCR

Updated January 2005

Table of Contents:

University of California, Riverside

Computing and Communications

Electronic Communications Policy (ECP) Overview and Implementation at UCR

Updated January 2005

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 routinely inspect, monitor, 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 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 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

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. policy).

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

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. policy).

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

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.).

UCR will provide information about back-up procedures to users of those services upon request.

VIII. Security

UCR attempts 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.

University of California, Riverside

Computing and Communications

Electronic Communications Policy (ECP) Overview and Implementation at UCR

Updated January 2005

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 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 Identify 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. Prior to PPS entries populating 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 AUTOMATIALLY 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 (@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 employees (that is all 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 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.