Faculty and Staff ECP Guidelines

Overview

UCR encourages the use of electronic information resources to conduct the University's business. The following is an abridged guide to the UC Electronic Communications Policy (ECP) which governs use of campus electronic resources including, but not limited to, computer labs, Webmail, iLearn, wireless network, proxy server, and virtual private network (VPN). By using UCR campus electronic resources you are agreeing to abide by the ECP. The complete version of the ECP, as well as the ECP Overview and Implementation at UCR, is available online at http://cnc.ucr.edu/index.php?content=policies.

Acceptable/Allowable Use of UCR Electronic Resources:

UCR electronic resources are primarily intended for instructional and research purposes, including class related activities, academic research, and administrative tasks that support instruction and research. For example, instructors may use iLearn to post class materials and interact with students. Staff may use the internet (network) to determine best price for purchasing University goods and services.

- ✓ ***Instructional and research related purposes***

- ✓ ***Public Service***

- ✓ ***Sending and receiving e-mail***; UCR Faculty and Staff may use campus electronic resources for sending and receiving email. This includes the use of Webmail, and the use of the campus network to access Webmail or other e-mail accounts. Use of campus resources for sending and receiving e-mail is limited by federal, state and local laws, as well as other University policies. E-mail activities that are prohibited include using UCR e-mail accounts or servers to send spam, for harassment, or for commercial purposes such as operating a business.

- ✓ ***Accessing the Internet; UCR*** Faculty and Staff may use campus Internet resources, including the wireless network and Internet access provided in various buildings. Access to the Internet is subject to individual departmental policies of the department providing the service, as well as federal, state or local laws, other parts of the ECP, or other University policies. Internet activities that are prohibited include using the UCR network to illegally download copyrighted materials such as movies or music, excessive bandwidth usage that is significant enough to adversely affect campus network performance, and deliberately or unknowingly spreading computer worms or viruses over the Internet.

- ✓ ***Incidental Personal Use***

Not Acceptable/Allowable Use of UCR Electronic Resources:

All relevant federal, state, and local laws apply when using University electronic communications. This includes laws that prohibit 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.

- ✓ ***Illegal activities***

- ✓ ***Violations of University policies***; All relevant University policies apply when using UCR electronic resources. This includes policies on sexual harassment, other forms of harassment, and intellectual property. For example, campus resources may not be used to obtain or re-distribute the intellectual property of others without authorization, including research, presentations, etc. Campus e-mail, iViews, and iLearn may not be used to send spam or other harassing e-mails. In addition, individual departmental resources may only be used in accordance with departmental policies.

- ✓ ***Use of electronic communications resources for commercial benefit or personal financial gain***; Campus electronic resources may not be used for commercial benefit or personal financial gain. For example, Faculty and Staff websites may not be used to sell products or services.

- ✓ ***Utilizing the University's name and/or seal without appropriate approvals***; Users of UCR electronic resources must abide by University policies regarding the use of the University's name, seal, or trademarks. The University's name, seal, or trademarks may not be used without appropriate authorization. For example, Faculty and Staff may not include the University Seal on personal web sites without authorization.

- ✓ ***Giving the impression that you 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;*** Users of campus electronic resources may 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. For example, the University name may not be included in advertisements for products or services without authorization to imply University affiliation or endorsement.

- ✓ ***Causing excessive strain on any campus electronic communications resource or unwarranted or unsolicited interference with others' use of electronic communications;*** 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. For example, campus electronic resources may not be used to send spam or engage in denial of service attacks. In addition, excessive bandwidth usage that adversely affects campus network services is prohibited and may result in restrictions on access.

What to Expect as an Electronic Communications User at UCR

Access and Access Restrictions

Duration of Access – Faculty and staff access to electronic communication services is dependent upon position and employment within the University. For visiting post-doctoral faculty, non-Academic Senate faculty, and staff, the account will be terminated 30 days after retirement or separation from employment. For Academic Senate faculty, the account will be terminated 90 days after separation from employment. A faculty member who retires completely from UCR will have a lifetime email account. A staff member who is involuntarily terminated will lose access immediately. It is important to remember that the email account is the property of the University, so an involuntarily terminated staff member's account may be viewed by their supervisor without consent.

Access Restrictions – Access to campus electronic resources may be restricted when there is substantial reason to believe that violations of law or University policies have taken place, or when time-dependent, critical operational circumstances exist. Violations of law or University policies include but are not limited to, excessive bandwidth use (enough to cause network performance degradation), continued off-campus complaints with no response from on-campus responsible parties, verified open proxy or open mail servers, attacks observed by Computing & Communications' network monitoring systems, and verified DMCA violations.

Backups and Data Retrieval – Electronic communications are routinely backed up. However, this is only for purposes of system integrity and reliability, in order to support data restoration in case of disk failure. It is not designed to provide for future information retrieval.

Policy Enforcement

Violations of the ECP may result in revocation of access to a single resource, a combination of resources, or all campus electronic resources, depending upon the violation.

UCR in general cannot 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.

Security, Confidentiality and Privacy

Because of core University principles relating to academic freedom and shared governance, freedom of speech and respect for privacy are important in the management and use of electronic resources. However, in general, electronic communications are no longer considered private if one party voluntarily shares the content with a campus official or manager of the computing system.

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 UC policy. UCR does not routinely inspect, monitor, or disclose electronic communications without the holder's 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:

- ✓ When it is required by and consistent with law.
- ✓ When there is substantiated reason to believe that violations of law or of University policies have taken place.
- ✓ 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 meet its teaching or research obligations.

Without at least one of those preceding criteria, there will be no non-consensual access to electronic resources. For example, if an employee is on vacation, the employee's supervisor would not be able to access his or her account without going through the extensive process of approval, and showing clearly how one of the four emergency criteria applies.

However, once employment is terminated, any content on the electronic resources remains as University of California property, and is no longer confidential.

References:
UCR Overview and Implementation of the Electronic Communications Policy
UC Electronic Communications Policy
Digital Millennium Copyright Act (DMCA)