

ADA Compliance

If you are responsible for electronic communications that are required for academic or administrative purposes, ensure that they are accessible to users with disabilities.

Administrative Records

Additional University policies apply to administrative records in electronic format whether or not they are communications records:

- Business & Finance Bulletin RMP-8 which describes the University's policies on privacy of and access to information
- Business & Finance Bulletin IS-3 which contains additional guidelines regarding the security of University records in electronic format

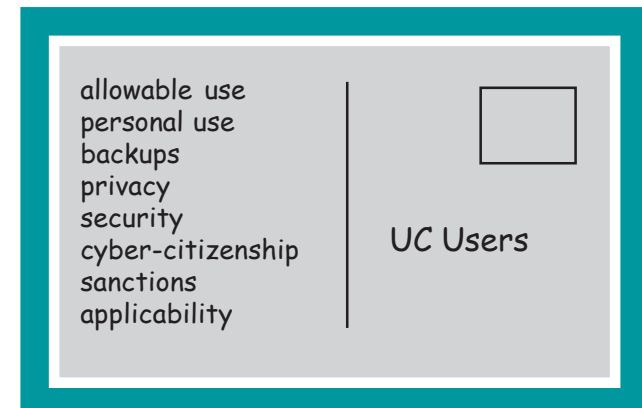
Systems Users

- Follow the University privacy guidelines in RMP-8
- Do not transfer critical University records or confidential records from secure to non-secure equipment or to insecure locations
- Observe all guidelines regarding the use of passwords and other security mechanisms
- Report violations of electronic information security guidelines

Proprietors and Custodians

If you are in charge of University administrative records in electronic format or have been assigned to protect them, you must comply with IS-3, *Electronic Information Security*. Implementing guidelines are available at <http://www.ucop.edu/ucophome/policies/bfb/is3guide.pdf>

Getting the Message



Highlights of the
University of California
Electronic Communications Policy
(including portions of Business & Finance Bulletin
IS-3, Electronic Information Security)

The ECP Applies to

The University of California Electronic Communications Policy applies to:

- All electronic communications resources provided by the University
- All users and uses of those resources and
- All University records in the form of electronic communications

Some of the electronic communications services covered by the Policy include: telephones, voicemail, interactive voice response systems, audio and video teleconferencing; electronic mail and mail services such as bulletin boards, mailing list systems, and newsgroups; electronic publishing services such as the web; and electronic broadcasting services such as radio, television, and webcasts.

Allowable Use

You may

- Create web sites and mail lists, send and receive email, make telephone calls, etc. for teaching, research, study and University business, including public service, and for incidental personal purposes
- With special authorization: host web sites and mail lists, convene video and audio teleconferences, webcast, and broadcast for teaching, research, study and University business but not for personal purposes

You may not

- Break the law—including laws against cyberstalking, copyright infringement, disrupting networks and systems, and tapping telephones
- Violate any University policy—including policies on sexual and other harassment, use of the University name and seal, and use of University facilities
- Disrupt network and systems operations, for example by transmitting viruses, sending spam, or hacking into others' transmissions or files

Security

Security measures are not infallible but you are safer with them than without them.

- Use passwords and other aids to protect material you want to keep private
- Do not share your accounts or passwords with others
- Use virus protection software provided by your department

Cyber-Citizenship

Spam, chain mail, massive mailings, denial of service attacks, transmission of viruses, and other types of misuse of services are prohibited.

The law prohibits the theft or abuse of computers and electronic resources. Abuses include:

unauthorized entry into, use or transfer of, or tampering with the communications of others, and interference with the work of others and with the operation of electronic communications resources, systems, and services

Some of these offenses are felonies. Thanks to your cooperation, most University electronic communications are problem-free.

Sanctions

Policy violations may lead to restriction of access to University electronic communications resources and/or disciplinary action up to and including dismissal.

Telephones

- Use of UC telephones creates transaction records that are reviewed as part of accounting procedures
- Announce your presence in conference calls but be aware that others may not do so
- Remember that conversations on speakerphones may be overheard

Backup and Retention

System back-ups are created to assure integrity and reliability. You can get information about back-up procedures for the electronic communications resources you use from the administrator of the service.

Be aware that systems operators are not required to retrieve electronic communications for individuals:

- Find out whether your department provides automatic back-ups for services you use
- Take responsibility for creating your own back up copies of communications you need to keep
- If you keep electronic records long-term, understand that you may need to transfer them to current electronic formats

More Information

The complete text of the Electronic Communications Policy is available online at

<http://www.ucop.edu/ucophome/policies/ec/>

The online Policy site has links to ECP implementing guidelines for the Office of the President.

- Bypass, disable, or remove a security mechanism applied by University system or network administrators
- Give the appearance that you represent the University if you are not authorized to do so
- Make it appear that the University endorses an outside organization when it does not
- Pretend to be someone else, e.g. by using someone else's email address
- Conduct a business not sponsored by the University
- Allow a third party or outside organization to use your accounts, network ID, or passwords
- Use your accounts on behalf of an outside organization not recognized by or affiliated with an academic or administrative unit of the University
- Release personal information about others to outside parties except under the special circumstances described in UC policies
- Break into private communications such as email, limited-access web sites, and phone conversations
- Refuse to produce University administrative records when asked by a University official

Guidelines for Personal Use

You may use some electronic communications services (such as telephones, email, and web sites) incidentally for personal purposes provided that the use does not:

- Interfere with others' use of those services
- Interfere with the work of University employees, including your own, and
- Incur noticeable, incremental costs to the University

But note:

- You are responsible for any loss or damage you may suffer because of personal use of UC electronic communications facilities
- Personal communications records stored on UC facilities might be treated as University records unless it is obvious that they are not

Privacy

Privacy and Access Without Consent

The University does not routinely monitor, inspect or disclose electronic communications. However, it may do so under four circumstances identified in the Policy:

- When required by and consistent with law
- When there is substantiated reason to believe that violations of law or certain University policies have taken place
- When there are compelling circumstances or
- Under time-dependent, critical operational circumstances

The Electronic Communications Policy requires that the Senior Vice President-Business and Finance authorize in advance any access to electronic communications records without the consent of the holder of the records. In emergency circumstances the records may be sought first and the action post-authorized.

University Privacy Guidelines

Privacy guidelines for electronic communications are based on Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information.

- Do not look at other people's electronic communication without permission
- Do not seek out or use personal information about other people
- Do not reveal, give or sell personal information about others to third parties
- Do not monitor or record telephone conversations without the consent of all participants or a court order

Privacy and Public Records Disclosure

- University records may be subject to disclosure under the California Public Records Act and are subject to UC records management policies
- Unlike electronic communications records held by employees, students' communications are presumed not to be University records

Privacy Cautions

The Web

- Personal information on open web pages is not private
- Even closed or unlinked web pages might be found by search engines
- When you access the web you create transaction records that may be reviewed by systems personnel
- Some web sites try to place small files ("cookies") on your computer that might help others track the web pages you access
- Web sites on University servers must tell users how to contact the owner or webmaster

Email, Lists, Newsgroups, and Bulletin Boards

- Systems personnel may inadvertently see the contents of email messages in the course of their duties
- If you send messages to open groups, your email address will become public
- Your University email address is a public record
- The University cannot protect you from receiving offensive communications
- When you send email, the recipients might forward it to others
- The contents of forwarded messages can be changed from the original
- Copies of email may remain on a backup system even after you have discarded the message