University of California Electronic Information Resources

User Agreement for the University of California Office of the President (UCOP)

Individuals who use University of California electronic information resources **must sign this agreement as a condition of access to those resources** indicating that they have read and understand the statements in this document and that they agree to comply with applicable policies and laws governing the use of electronic information resources and the protection of data privacy. The user agreement is available online.

The University may provide employees, independent consultants/contractors, and other individuals access to electronic information resources to carry out their responsibilities to the University. These resources can include:

- computers
- telecommunications devices, voicemail, and fax machines
- smartphones and PDAs
- video and audio equipment
- e-mail and electronic calendars
- Internet (e.g., the web) and UCOP network access
- systems access

The University reserves the right to restrict or rescind access to these resources at its discretion.

Individuals are required, as a condition of being granted use of and access to University electronic information resources,

- to abide by University policies that govern use of these resources,
- to protect and maintain the privacy and confidentiality of University information to which they have access,
- and to disclose confidential information only under certain conditions allowed by University policy.

Use of UCOP Electronic Information Resources

Users are expected to abide by all applicable policies and laws when using University electronic information resources. Users are held accountable for misuse and are disciplined in accordance with applicable University human resources policies. Examples of misuse include but are not limited to the activities in the following list:

- Violating any applicable state or federal law or regulation
- Using resources for personal financial gain or non-University commercial purposes
- Accessing resources for personal use so that the University incurs noticeable, incremental costs through lost productivity, direct charges, or interference with University operations
- Using e-mail for unauthorized mass messaging, such as distribution of chain or spam e-mail messages, which causes excessive strain on electronic communications resources
- Sharing or providing access to resources, such as University-issued computers, with unauthorized individuals
- Installing unauthorized software or equipment
- Disclosing confidential or sensitive information without consent or authorization

- Violating policy or measures intended to ensure network, computer, and data security and to safeguard against theft or loss
- Violating copyright law, such as sharing copyrighted electronic material without permission or otherwise engaging in illegal filesharing activities
- Violating terms of software licensing agreements
- Creating a hostile work environment
- Using a departmental or functional e-mail account (e.g., deptname@ucop.edu or assistant@ucop.edu) or mailing list (e.g., Listservs) for unofficial or unauthorized purposes
- Assuming a false identity, or masking the identity of an account or machine without permission
- Implying University endorsement of a product, service, or statement of a non-University entity without approval
- Giving the impression, without authorization, of representing a position, giving opinions, or making statements on behalf of the University or a University unit
- Using the University's name or seal without appropriate authorization

Access to Electronic Communications Records

The University of California Electronic Communications Policy (ECP) governs access to electronic communications records.

Monitoring of Content

As a general policy matter, the University does not monitor the content of electronic communications without the user's consent. However, users should be aware that access to and inspection of electronic communications (including e-mail) *may be granted or required* under certain conditions as set forth in the ECP (for example, where there is reason to believe a law has been violated, or when there is a critical time-sensitive operational need). The ECP's procedures for nonconsensual access will be followed where necessary. Users should also be aware that access to, inspection of, and preservation of relevant electronic communications (including e-mail) is *required by federal law* when the University reasonably anticipates that a lawsuit may be filed against it or is engaged in legal action.

Unplanned Absences or Separation

Users are advised that in the case of an unplanned, extended absence, the University may find it necessary to access an individual's electronic communications in order to ensure business continuity. Such access will be conducted with the least perusal of contents possible, per the ECP. The individual will be informed of the access upon return to work. After an individual separates from the University, the University may access electronic communications records for business purposes and may destroy electronic files, including e-mail.

Protection of Personal or Confidential Information

Access to University information, including data records, is authorized for University employees or other users when necessary for them to perform assigned duties. Such use must be in accordance with assigned duties. The University electronic information resources, including corporate systems, to which users are provided access may contain information or data records pertaining to members of the University of California that are defined as personal or confidential under University policy and the State of California Information Practices Act of 1977 (IPA). The IPA applies to virtually all University records containing personal or confidential information and is intended to protect the privacy of individuals about whom records are maintained. Personal information about students is protected pursuant to the federal regulations implementing the Family Education Rights and Privacy Act of 1974 (FERPA), and the University of California Policies Applying to Disclosure of Information from Student Records. These policies preclude the intercampus exchange of confidential student data except in limited circumstances.

Individuals provided access to confidential or other sensitive information must take measures to safeguard it from unauthorized access, release, or disclosure. Examples of frequently used personal data elements

that must be protected include gender, ethnicity, home address and telephone number, date of birth, income tax withholding data, citizenship, Social Security number, and personal health information. Some examples of confidential business information that must be protected include performance evaluations, peer reviews, negotiation details, and risk management information.

Mobile Device Usage Agreement

Per UC policy, Business and Finance Bulletin G-46, Guidelines for the Purchase and Use of Cellular Phones and Other Portable Electronic Resources (PDF), any users issued University-provided portable electronic communications equipment and/or services agree to the following terms:

- The equipment/service will be used primarily for official University business.
- Any personal use will be incidental in nature, and the user will reimburse the University for personal use that results in noticeable incremental costs to the University.
- All records related to the purchase, use, and disposition of the equipment or service, including cell phone or other service statements, are the property of the University and subject to disclosure under the California Public Records Act.
- The user will immediately report the loss or theft of the equipment to the IT Service Desk.
- The user will be responsible for safeguarding and controlling use of the equipment, including any data on it.
- The user will comply with UCOP minimum security standards to protect the equipment and data.
- The user will return the equipment and/or the University will stop paying for the service if there is no longer a business need, or if the user separates from University employment.

Relevant University Policies

- University of California Electronic Communications Policy
- Policies Applying to the Disclosure of Information from Student Records (PDF)
- RMP-7, "Privacy of and Access to Information Responsibilities" (PDF)
- RMP-9, "Guidelines for Access to University Personnel Records by Government Agencies:"
    - RMP-9a (PDF)
    - RMP-9b (PDF)
    - RMP-9c (PDF)
- Guidelines for Purchase and Use of Cell Phones and Other Portable Electronic Resources (PDF)
- UC Personnel Policies for Staff Members 62
- Collective Bargaining Agreements
- Use of E-mail at UCOP
- Acceptable Use of UCOP Electronic Information Resources
- UCOP IT Policies

Agreement and Signature

I agree to comply with University policies and state and federal laws and regulations, as described above, regarding the use of University electronic information resources and the protection of sensitive data.

_____ _____

Signature of User **Date**

_____ _____

Print User Name **User's Telephone Number**

A copy of the signed agreement should be provided to the user. For employees, the original signed agreements must be kept in the personnel files. For consultants/contractors and others, the original must be retained by the department that sponsored the individual's access.