What does privacy mean at UC?

Privacy consists of (1) the individual's ability to conduct activities without concern of or actual observation and (2) the appropriate protection, use, and release of information about individuals. The University must balance its respect for both types of privacy with its other values and with legal, policy, and administrative obligations.

Academic and intellectual freedoms are values of the academy that help further the mission of the University. These freedoms are most vibrant where individuals have autonomy: where inquiry is free because it is given adequate space for experimentation and the ability to speak and participate in discourse within the academy is possible without intimidation.

Transparency and accountability are values that form the cornerstone of public trust. Access to information concerning the conduct of business in a public university and an individual's access to information concerning him/herself is a right of every citizen as stated in the California Constitution.

The University of California, Santa Cruz is committed to upholding each individual's right to personal privacy as articulated by the Information Practices Act of 1977. Every member of the campus community involved in the collection, maintenance, disclosure, or disposition of personal information is obligated to be informed of and comply with various laws, regulations, and university policy governing privacy.

Useful References

• UC Privacy Policies and References (http://www.ucop.edu/ethics-compliance-audit-services/compliance/privacy/privacy-policies-and-references.html)

• Rules of Conduct for University Employees Involved with Information Regarding Individuals (http://www.ucop.edu/ethics-compliance-audit-services/_files/compliance/privacy/rules-of-conduct.pdf)

• Information Practices Act, Civil Code 1798 et seq.

• Generally Accepted Privacy Principles, AICPA

• Family Education Rights and Privacy Act (FERPA)- Office of the Registrar

• CA Attorney General Privacy Enforcement and Protection

RULES OF CONDUCT FOR UNIVERSITY EMPLOYEES INVOLVED WITH INFORMATION REGARDING INDIVIDUALS

A. Employees responsible for the collection, maintenance, use, and dissemination of information about individuals which relates to their personal life, including their employment and medical history, financial transactions, marital status and dependents, shall comply with the provisions of the State of CA Information Practices Act.

B. Employees shall not require individuals to disclose personal or confidential information about themselves which is not necessary and relevant to the purposes of the University or to the particular function for which the employee is responsible.

C. Employees shall make every reasonable effort to see that inquiries and requests by individuals for their personal or confidential records are responded to quickly, courteously, and without requiring the requester to repeat the inquiry to others unnecessarily.

D. Employees shall assist individuals who seek information pertaining to themselves in making their inquiries sufficiently specific and descriptive so as to facilitate locating the records.

E. Employees shall not disclose personal or confidential information relating to individuals to unauthorized persons or entities. The intentional disclosure of such information to such persons or agencies may be cause for disciplinary action.

F. Employees shall not seek out or use personal or confidential information relating to others for their own interest or advantage. The intentional violation of this rule may be cause for disciplinary action.

G. Employees responsible for the maintenance of personal and confidential records shall take all necessary precautions to assure that proper administrative, technical, and physical safeguards are established and followed in order to protect the confidentiality of records containing personal or confidential information.

UNIVERSITY OF CALIFORNIA, SANTA CRUZ

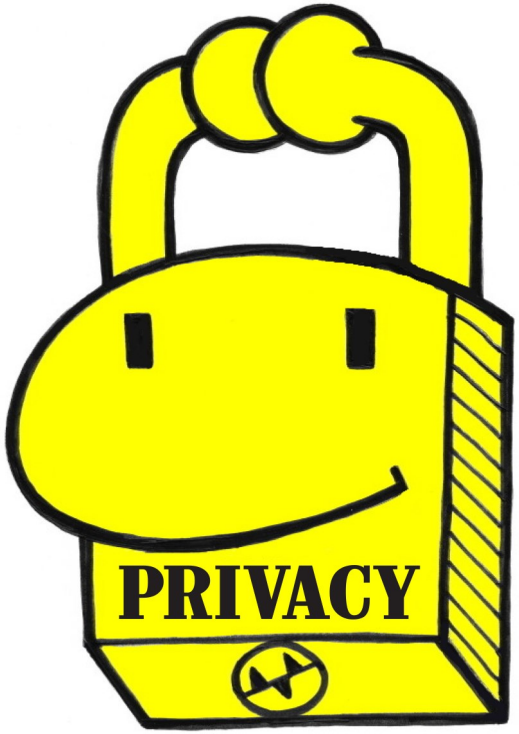
Privacy and Information Practices
Office of Campus Counsel
infopractices.ucsc.edu privacy.ucsc.edu

831.459.4003 pra@ucsc.edu privacy@ucsc.edu

August 2023

UNIVERSITY OF CALIFORNIA, SANTA CRUZ

Privacy and Information Practices



Key Concepts and Best Practices

Information Privacy Principles

KEY CONCEPTS

• **NOTICE** Collection documents must include notice identifying purpose for which information is collected and used

• **ACCURACY** Reasonable steps shall be taken by the collector to ensure the information is accurate, complete, up-to-date, and relevant to the purpose for which information is collected

• **USE** Personal information shall not be used or disclosed other than for purposes collected, except with consent of the individual or when required by law

• **ACCESS** Except under express provisions of the law, an individual shall be permitted to inspect all personal information in any record containing personal information that is maintained by reference to that individual

• **AMENDMENT** An individual has a right to request in writing an amendment of a record

• Sensitive personal information generally requires an extra level of protection and P3 and P4 classified information requires a higher duty of care

• Collection of personal information shall be limited to that which is necessary for lawful purposes directly related to a function or activity of the collector

• Individuals who have access to or control of personal information, whether electronic or hardcopy, must safeguard the information against loss, unauthorized access, use, modification or disclosure

• To the greatest extent possible, personal information should be collected from the individual to whom the information pertains

• Access to and use of personal information shall be limited to legitimate business purposes and directly connected to the purpose for which it was collected.

• Personal information must not be used for commercial purposes

BEST PRACTICES

• Apply privacy principles to everyday work

• Determine whether information is necessary and relevant to document/process

• Adopt "clean desk" practices; secure documents in locked cabinets; lock computer when unattended (even temporarily)

• Do not include restricted information on payment documents (post travel, direct pay, etc)

• When SSN is requested to confirm identity, use last four digits only

• Inform vendors SSN is not required on invoices

• Establish password access to databases containing personal and restricted information

• Ensure data is encrypted if electronic systems are unsecure and do not use unsecure email to transmit, instead securely transmit documents with **Virtru**

• Do not scan documents containing restricted information using unsecure scanner

• Do not store documents containing restricted information if not 'Office of Record'

• Follow disposition policies -- Personal information must be disposed of in a secure manner, e.g. by shredding or via secure service -- do not recycle or place in trash receptacle

• Ensure personal information is removed from computers, hard drives, USB devices, etc. prior to equipment reuse/disposal

• Report suspected information security breach immediately to supervisor, Information Practices, and ITS (hard copy and electronic)

• Avoid "shoulder surfers"

P4 INFORMATION

1. Electronic manifestation of an individual's first name or first initial, and last name, in combination with one or more of the following:
   - ♦ Social Security number (SSN)
   - ♦ Drivers license number or State-issued Identification Card number
   - ♦ Account number, credit or debit card number in combination with any required security code, access code, or password that could permit access to an individual's financial account
   - ♦ Medical information, including any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional
   - ♦ Health insurance information, including an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records
2. Electronic protected health information (ePHI) protected by Federal HIPAA legislation
3. Credit card data regulated by the Payment Card Industry (PCI)
4. Information relating to an ongoing criminal investigation
5. Court-ordered settlement agreements requiring non-disclosure
6. Both encrypted personal information and the encryption key or security credential that would render such personal information readable or useable.

The Information Practices Act, Civil Code Section 1798 et seq., defines personal information as "...any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual."