BFB-RMP-7: Protection of Administrative Records containing Personally Identifiable Information

Responsible Officer:	Chief Information Officer & Vice President – Information Technology Services
Responsible Office:	IT – Information Technology Services
Issuance Date:	9/16/2019
Effective Date:	9/16/2019
Last Review Date:	8/21/2019
Scope:	This applies to all University Employees, students and others who have authorized access to Administrative Records containing Personally Identifiable Information at all Locations.

Contact:	Laurie Sletten
Title:	UC Records Manager
Email:	Laurie.Sletten@ucop.edu
Phone #:	(510) 987-9411

TABLE OF CONTENTS

I. POLICY SUMMARY

The University of California respects the privacy of individuals as fundamental to its mission and a value enshrined in the California constitution. Privacy:

1. Is essential to promoting the values of academic and intellectual freedom,
2. Plays an important role in upholding human dignity and safeguarding a strong, vibrant society, and
3. Serves as the basis for an ethical and respectful workplace.

The University is committed to protecting personal privacy in its operations, activities, and management of information. The University must balance this commitment with other important commitments, including public accountability and the right of people to access information about the conduct of the public's business. This policy outlines the requirements and processes for ensuring the University protects Personally Identifiable Information found in Administrative Records by meeting its legal obligations, as well as balancing information privacy and autonomy privacy with competing institutional obligations, values, and interests.

The purpose of this bulletin is to establish the systemwide processes for safeguarding personally identifiable information in Administrative Records. When Personally Identifiable Information is requested, the University must examine whether its disclosure or use is governed by law, University policy or contract, and if not, whether disclosure or use constitutes an unwarranted invasion of personal privacy. If the University's response to the request is not mandated by law, policy, or contract, the requested Personally Identifiable Information may be released, used or disclosed only after a balancing analysis determines that it does not constitute an unwarranted invasion of personal privacy.

This policy is for use by anyone in the University community who makes decisions about Administrative Records. Material provided in the procedures may be helpful to anyone in the institution who creates or receives records of any type.

II. DEFINITIONS

Administrative Records: As defined in Business and Finance Bulletin Records Management and Privacy-1: University Records Management Program (RMP-1), this term is used to describe any record, regardless of physical form or characteristics, that documents or contains valuable information related to the organization, functions, policies, decisions, procedures, operations, or other business activities of the University.[1]

California Information Practices Act (IPA): The law that guarantees the right of

[1] Administrative records do not include the records held by the Principal Officers of The Regents; teaching and research records (e.g., library materials, faculty research and teaching materials, student examinations); or records pertaining to individual patient care (medical records).

access to records containing an individual's personal information, with certain limitations, e.g. in centralized files with their name or other identifier, and sets forth provisions to govern the collection, maintenance, accuracy, dissemination, and disclosure of information about them. Special procedures for providing access to and protecting the privacy of University records containing personal data are required by the IPA.

California Public Records Act (CPRA): The law that provides public access to state and local agency records relating to the conduct of the public's business. Public records must be disclosed upon request, unless a statutory exemption applies. In providing access, CPRA remains mindful of individual privacy rights.

Campus Privacy Official: The individual at each location responsible for overseeing the strategic direction and application of the UC Statement of Privacy Values & Privacy Principles[2] and UC Privacy Balancing Process.

Commercial Purposes: Any purpose that has financial gain as a major objective.

Employee: Faculty, staff, or any other **workforce member**, volunteer, contractor, researcher, student worker, student supporting/performing research, medical center staff/personnel, clinician, student intern, student volunteer, or person working for UC in any capacity or other augmentation to UC staffing levels.

Family Educational Rights and Privacy Act (FERPA): The federal law that addresses the privacy of students' educational records, which are records directly related to a student and are maintained by the University or a party acting for or on behalf of the University.

General Data Protection Regulation ("GDPR"): A privacy law of the European Union that governs the use of personal data. It concerns the personal data of individuals in the European Economic Area (EEA), which includes EU countries as well as the United Kingdom, Iceland, Norway, and Lichtenstein. The GDPR defines "personal data" very broadly such that the term includes names, addresses, phone numbers, national IDs, IP addresses, profile pictures, personal healthcare data, educational data, and any other data that can be used to identify an individual. It addresses multiple issues, such as the rights of data subjects, consent, and purpose of use.

Information Practices Coordinator: The individual at each location responsible for administering responses to records requests, and providing guidance to constituents at their locations on matters related to the access, use, and disclosure of information maintained in Administrative Records.

Information Privacy: As defined in the UC Statement of Privacy Values & Privacy Principles, is the appropriate protection, use, and dissemination of information about

[2] For more information, see Section IV.C. Roles and Responsibilities. A list of current privacy officials can be found at http://www.ucop.edu/ethics-compliance-audit-services/compliance/privacy/campus-privacy-officials.html

individuals.

Location: A discrete organization or entity governed by the Regents of the University of California. Locations include, but are not limited to: campuses, laboratories, medical centers and health systems, as well as satellite offices, affiliates, or other offices controlled by the Regents of the University of California.

Mailing Lists: Any compilation of names and addresses, including email addresses.

Personally Identifiable Information (PII): Any information that describes or identifies an individual, including but not limited to name, Social Security number, physical description, home address, telephone numbers, email address, education, financial matters, medical or employment history, or statements made by or attributed to the individual. This is not an exhaustive list. Other elements that identify an individual may be included.

Privacy and Information Security Board: The privacy and information security board at each location that advises on privacy and information security; sets strategic direction for autonomy privacy, information privacy, and information security; champions the UC Privacy Values & Privacy Principles, and the UC Privacy Balancing Process; and monitors compliance and assesses risk and effectiveness of location privacy and information security programs. These boards may be separate committees or structured as part of an existing location governance committee.

Records Management Coordinator: As defined in RMP-1, the individual at each location responsible for the development, coordination, implementation, and management of the Records Management Program at the location.

Records Management Program: In accordance with RMP-1, the Program that promotes sound, efficient, and economical records management in the following areas: (1) creation, organization of, and access to records; (2) maintenance and retention of Administrative Records; (3) security and privacy of records; (4) protection of records vital to the University; (5) preservation of records of historical importance; (6) disposition of Administrative Records when they no longer serve their purpose; and (7) other functions the University may deem necessary for good records management.

Student Applicant Records: Records of a person during the period of application, acceptance, and admission to the University, *prior* to enrollment.

Telephone Directories: A collection of individuals' names, telephone numbers, and other contact information, including employee (campus) or student directories.

UC Privacy Balancing Process: The process designed to address privacy risks when there is no policy in place pertaining to the situation.[3]

[3] See UC Privacy and Information Security Steering Committee Report to the President January 2013, page 18

III. POLICY TEXT

This policy applies to all Personally Identifiable Information (PII) in the University of California's Administrative Records, regardless of the record's function or medium, and addresses requirements related to the treatment of such information. Requests for academic personnel records from government agencies are governed by Business and Finance Bulletin Records Management and Privacy Policies 9a, 9b, and 9c.[4]

All Employees and other individuals associated with the University who have access to Administrative Records containing PII must understand their responsibilities for safeguarding the privacy of that information. The Information Practices Coordinators, Campus Privacy Officials, and Records Management Coordinators in consultation with the UC Office of the General Counsel (OGC), are responsible for providing overall policy and procedural guidance to University locations about privacy of and access to Administrative Records.[5]

A. Rules of Conduct for Employees with Access to Information Concerning Individuals

The University of California requires Employees to adhere to the following rules of conduct concerning minimum standards[6] for the collection, maintenance, disclosure, safeguarding, and destruction of Administrative Records containing PII. The California Information Practices Act (IPA) requires that any officer or employee who intentionally violates this policy, including these rules of conduct, may be subject to disciplinary action.[7]

1. Employees responsible for the collection, maintenance, use, and dissemination of Administrative Records that contain PII, must comply with the provisions of the IPA.
2. Employees must not require individuals to disclose PII about themselves or others that is not necessary and relevant to the purposes of the University or to the particular function for which the employee is responsible.
3. Employees must make every reasonable effort to ensure inquiries and requests by individuals for records containing their PII are responded to quickly, courteously, and without requiring the requester to repeat the inquiry to others unnecessarily.
4. Employees must assist individuals seeking information pertaining to themselves with making their inquiries sufficiently specific and descriptive to facilitate locating the records.

[4] For additional requirements concerning requests for and access to academic peer review records, see policy APM-160.
[5] For more information about the specific responsibilities of each role, *see* Section IV.C.
[6] See Rules of Conduct for University Employees Involved with Information Regarding Individuals, part of the Privacy Principles and Practices at UC
[7] California Civil Code § 1798.55

5. Employees must not disclose PII to unauthorized persons or entities.
6. Employees must not seek out or use PII relating to others for their own interest or advantage.
7. Employees responsible for the maintenance of records containing PII must take all necessary precautions to assure that proper administrative, technical, and physical safeguards are established and followed in order to protect the records from unauthorized access, use and disclosure.

B. Management of Records Containing PII

All locations must follow the requirements below:

1. Collection of Information

The University should only collect and maintain information that is necessary and pertinent to accomplish its University mission.

To the greatest extent practicable, information about an individual must be collected directly from the individual to whom it pertains. When this is not possible, the University must maintain the source or sources of information, in a readily accessible format, in order to provide the source or sources to the individual upon request. When PII is disclosed, individuals may be notified according to existing legal requirements, University policy, and location practices.

2. Procedures for Individuals' Rights Related to Records about them

Each location must establish procedures that ensure an individual's right to inquire and be notified whether the University maintains records about them; and provide the records for inspection by the individual to the extent required by law. These procedures must be consistent with the requirements of the IPA, and University policies, such as UC IS-3 Electronic Information Security.

3. Use of PII for Commercial Purposes

Employees responsible for maintaining or accessing records with PII must not distribute, sell, or rent PII for commercial purposes unless such action is specifically authorized by law.[8]

4. Disposition of Administrative Records Containing PII

Information held by the University must be disposed of in accordance with federal and state law, and as required by RMP-2 Records Retention and Disposition and the UC Records Retention Schedule, unless it is needed as evidence in an investigation, foreseeable or on-going litigation, on-going audit, on-going records request or other special circumstance – in which case the information must be retained until these actions have been completed or resolved.

5. Procedures for Reporting Unauthorized Disclosures of PII

Each location is responsible for developing its procedures for reporting

[8] For example California Civil Code §1798.60

unauthorized disclosures of PII for both paper and electronic records. Procedures for reporting electronic unauthorized disclosures of PII must be consistent with the Location Incident Response plan[9].

6. **General Data Protection Regulation ("GDPR") Requirements**

   GDPR requirements may be more restrictive and the location's Privacy Official may be consulted for guidance.

   For specific procedures concerning mailing lists and student records including application records, see Section VI Procedures. For information concerning academic peer review records, see APM-160.

C. Evaluating Use or Disclosure of PII

When law, policy, or contract does not provide definitive guidance regarding a proposed use or disclosure of PII, the location must use the UC Privacy Balancing Process to adjudicate privacy and other competing interests.

Under the Balancing Process, the location must not make public disclosures of information unless it can demonstrate that the interests served by disclosure outweigh the individual's privacy interest. In reaching this decision, the location must review specific statutory exceptions that might allow for disclosure of PII. Situations involving unprecedented and significant balancing concerns are referred to the location's Privacy Board unless a relevant alternative adjudication path is already established.

IV. COMPLIANCE / RESPONSIBILITIES

A. Implementation of the Policy

The Vice President for Information Technology Services and Chief Information Officer is responsible for issuing and updating any requirements, standards or guidelines that support this policy.

Chancellors, the Vice President of Agriculture and Natural Resources, and UC Managed Laboratory Directors are responsible for designating an Information Practices Coordinator, Campus Privacy Official, and Records Management Coordinator to administer and implement this policy at their location.

The UC Information Practices Coordinator, UC Privacy Manager, and UC Records Manager facilitate regular communication among local Information Practices Coordinators, Campus Privacy Officials, and Records Management Coordinators to address consistent implementation of this policy throughout the University. Each Information Practices Coordinator, Privacy Official, and Records Management Coordinator must work together at their locations to ensure consistent implementation of this policy, as necessary.

[9] See the UC Incident Response Standard.

B. Revisions to the Policy

The Vice President for Information Technology Services and Chief Information Officer has the authority to initiate policy revisions and is responsible for regular reviews and updates consistent with approval authorities and applicable Bylaws and Regents' policies.

C. Roles & Responsibilities

The following functions are critical to ensuring the University handles information in a manner consistent with the University's legal obligations, policy requirements, and the UC Statement of Privacy Values & Privacy Principles. Together, Information Practices Coordinators, Campus Privacy Officials, and Records Management Coordinators serve as subject matter experts and collaborate with other disciplines to strengthen the University's information governance framework.

1. University Employees

All Employees and other University community members with access to records with PII must safeguard the records from unauthorized access, use and disclosure.

2. University Managers

All managers must ensure that Employees who have access to records with PII are made aware of their responsibilities for handling such records, including protecting the records from unauthorized access, use and disclosure.

3. Information Practices Coordinators

The Information Practices Coordinator at each location is responsible for administering responses to records requests, and providing guidance on matters related to the access, use, and disclosure of information maintained in Administrative Records. The California Public Records Act (CPRA) Office within the OGC provides guidance to campuses and may manage multi-campus CPRA requests on behalf of the locations. At their locations, Information Practices Coordinators also:

i. Ensure that procedures and practices for access, amendment, use and disclosure of Administrative Records adhere to federal and state laws, including but not limited to the IPA and the CPRA.

ii. Develop guidelines, including training programs, on IPA and CPRA practices, including the rules of conduct outlined in Section III.A.

iii. Review local PII collection and notice practices upon request.

iv. Assist with interpretation of federal and state privacy and disclosure laws and University policies including but not limited to the CPRA, IPA and the UC rules of conduct outlined in Section III.A.

4. Campus Privacy Officials

Campus Privacy Officials at each location are responsible for overseeing the strategic direction and application of the UC Statement of Privacy Values &

Privacy Principles, and UC Privacy Balancing Process throughout the activities at that location.

5. **Records Management Coordinators**

   As defined in RMP-1, Records Management Coordinators are responsible for the development, coordination, implementation, and management of the Records Management Program at their locations.

6. **Chancellors, the Vice President of Agriculture and Natural Resources, and UC Managed Laboratory Directors**

   These positions are responsible for designating an Information Practices Coordinator, Campus Privacy Official, and Records Management Coordinator to administer and implement this policy at their locations.

7. **The Vice President for Information Technology Services and Chief Information Officer**

   This position is responsible for issuing and updating any requirements, standards or guidelines that support this policy.

V. PROCEDURES

For specific categories of PII, all locations must follow the procedures below to ensure consistency across the University.

A. Student Applicant Records

In accordance with California law, the University only collects information relevant to the University's purposes. Disclosure of this information must be in accordance with state and federal law.

Until an applicant has enrolled in an academic program, any records referring to them are considered student applicant records and must be used and accessed in a manner consistent with the protections afforded by the IPA.

Records directly related to an enrolled student, including the student's applicant records, are subject to the Family Educational Rights and Privacy Act (FERPA).[10]

An applicant has the right to inspect records that reference them in relation to the application process, and are maintained in the applicant's file, with the exception of recommendation letters and associated records created with the documented understanding of confidentiality.[11]

1. Parents of Applicants

   In accordance with the IPA, the University must not release information from the applicant's records to the applicant's parents without the applicant's written

[10] For policy requirements and further information about privacy and potential disclosure of student records, please read Policies Applying to the Disclosure of Information from Student Records (UC PACAOS-130**)**
[11] California Civil Code §1798.38; 20 USC § 1232g(a)(1)(C)

consent, regardless of the individual's age or financial status. The University's current admissions process provides the opportunity to furnish this consent.

In accordance with FERPA, the University must not release student records (including application records) to parents without the student's written consent, regardless of age or financial status, unless such release falls under a specific exception under FERPA.

2. Third Parties

   In accordance with state law, the University may disclose PII about a University applicant to certain third parties (e.g., high school counselors). This information may include eligibility status or lack of certain grades. The University may disclose this information only if:

   a. The applicant gives prior written consent; or

   b. The disclosure is compatible with the original collection purpose, and if disclosure is made to an agency it is necessary for the agency to perform its constitutional or statutory duties; or

   c. The requested information will be used for scientific or statistical research and assurances of confidentiality and protection of personal identity are guaranteed; or

   d. As required or permitted by state or federal law.

3. Advancement, Development, and Alumni Office Staff

   Advancement, Development, and Alumni office Employees have legitimate educational interest in applicants' records. These offices may access applicant information, including PII, when the information is relevant and necessary to carry out their assigned duties and is clearly related to the purpose for which the information was originally collected.

B. University Mailing Lists and Telephone Directories

Upon written request from any individual, any University office that maintains a Mailing List must remove that individual's name and address from such list, unless the list is used by the University solely for necessary direct contact with the individual.

The University must not use or disclose its Telephone Directories and Mailing Lists for commercial purposes, unless such action is specifically authorized by law.

VI. RELATED INFORMATION

Academic Personnel Manual

- Section 160, Maintenance of, Access to, and Opportunity to Request Amendment of Academic Personnel Records

Business and Finance Bulletins

- IS-3, Electronic Information Security

- RMP-1, University Records Management Program
- RMP-2, Records Retention and Disposition
- RMP-9a, -9b, -9c, Guidelines for Access to University Personnel Records by Governmental Agencies

Personnel Policies for Staff Members

- PPSM 21, Selection and Appointment

Federal and State Laws

- California Constitution, Article I, Section 1 and 3
- California Information Practices Act
- California Public Records Act
- Family Educational Rights and Privacy Act

Other Presidential Policies and Guidelines

- Electronic Communications Policy
- Gramm-Leach-Bliley Compliance Plan
- UC Policy on Public Disclosure of Compensation Information
- UC Privacy Balancing Process
- UC Privacy and Information Security Steering Committee Report to the President January 2013
- UC Statement of Privacy Values & Privacy Principles

Other

- UC Procurement Appendix DS — Data Security and Privacy
- IS-3 Standards
- UC Incident Response Standard
- UC Institutional Information and IT Resource Classification Standard
- UC Institutional Information Disposal Standard

For specific additional requirements about Student Records, Protected Health Information (PHI), and Academic Peer Review Records please refer to the policies below:

- Student Education Records: UC PACAOS-130 Policies Applying to the Disclosure of Information from Student Records and the Federal Family Educational Rights and Privacy Act (FERPA) primarily govern the handling of student education records.
- Protected Health Information: The University's HIPAA policies, the Health Information Portability and Accountability Act of 1996 (HIPAA), and subsequent

amendments in the Health Information Technology for Economic and Clinical Health (HITECH) Act govern the handling of Protected Health Information.

- Academic Peer Review Records: See APM 160-20

  This policy defines the rights of individuals and entities to have access to academic peer review records.

VII. REVISION HISTORY

September 16, 2019: Major revision to update policy and combine outdated policies RMP-7, 11 and 12.

- Limited scope to personally identifiable information in administrative records.
- Identified areas of the old policies that are still relevant.
- Identified areas that needed updated content.
- Built on foundation of UC Statement of Privacy Principles & Values
- Defined GDPR and identified that it is not addressed in this policy
- Clarified roles of subject-matter experts
  - Privacy Officials
  - Records Management Coordinators
  - Information Practices Coordinators

This Policy was also reformatted to meet Web Content Accessibility Guidelines (WCAG) 2.0.

This policy replaces the following policies:

- BFB-RMP-7: Privacy of and Access to Information Responsibilities. November 1, 1985 Initial Version.
- BFB-RMP-8: Requirements of Privacy of and Access to Information. November 13, 2015 Rescinded.
- BFB-RMP-11: Student Applicant Records. June 15, 1989 Initial Version.
- BFB-RMP-12: Guidelines for Assuring Privacy of Personal Information in Mailing Lists and Telephone Directories. June 15, 1989 Initial Version