University of California, Merced

Access to Student Data

Responsible Official:	University Registrar
Responsible Office:	Office of the Registrar
Issuance Date:	August 8, 2017
Effective Date:	August 8, 2017
Summary:	This policy describes the conditions, and establishes procedures, under which student data may be distributed by Institutional Research and Decision Support (IRDS) and the Office of the Registrar.
Scope:	This policy applies to all UC employees and others using and disposing of University resources.

Contact:	Laurie Herbrand, University Registrar
Email:	lherbrand@ucmerced.edu
Phone:	(209) 658-0693

I. REFERENCES AND RESOURCES

Federal Laws and Regulations

- Family Educational Rights and Privacy Act (FERPA)
- Solomon Amendment & FERPA

State Laws and Regulations

- California Education Code Section 49073-49079.7

UC Policies

- UC Electronic Communications Policy
- IS-3 Electronic Information Security
- UC Appendix - Data Security and Privacy
- BFB-RMP-2: Records Retention and Disposition: Principles, Processes, and Guidelines

Guidelines/Resources

- Guidance on FERPA (Office of the Registrar)
- FERPA General Guidance for Students (Department of Education)
- Guidelines on Use of Mass Communications (Email) Services
- UC Merced Directory
- Institutional Research & Decision Support (IRDS)
- University of California Information Center

- National Student Clearinghouse
- Survey Coordination
- Data Request

II. POLICY / PROCEDURE SUMMARY & SCOPE

This policy sets forth the conditions, and establishes procedures, under which student data may be distributed by Institutional Research and Decision Support (IRDS) and the Office of the Registrar in a manner that is consistent with the Family Educational Rights and Privacy Act (FERPA) and established University policies.

This policy applies to all UC employees and others using and disposing of University resources.

III. DEFINITIONS

Definition of Student Data: Collected for official University Business, student data include any data collected and stored in the Banner Student Information System (SIS) for both admitted and registered students. Student data include information that may be passed to a downstream database or application, whether owned or contracted by the University of California, including student directory data as defined by FERPA and UC Merced policies. Distribution of data refers to UC Merced student data in any format, including hard copy, electronic format, and data in officially approved repositories (e.g., Campus Data Warehouse or centrally supported enterprise applications).

Aggregate Data: Aggregate data are defined as data that exclude identifying information such as student names and/or UC Merced identification numbers. Aggregate data are only provided for use in institutional analysis to campus officials with a legitimate educational interest. Reports of aggregate data produced for internal audiences are not to be reproduced, published, publicly posted, or used for any secondary purpose without the knowledge and approval of IRDS or the Office of the Registrar. Any data value less than 5 will not be included in any report.

Research: The systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.

Business Purpose: Refers to any data request for educational or research purposes.

Institutional Information Proprietor: Responsible person for establishing and documenting rules for use of, access to, approval for use, and removal of access to the Institutional Information related to their area of responsibility.

IV. POLICY TEXT

A. Requesting Student Data

1. Requests for student data are evaluated on a case by case basis and are either approved or denied by IRDS or the University Registrar. All data requests, whether originating from academic, research or administrative units are initiated by completing the Data Request online form located on the Office of Registrar

webpage. The timeliness of the review will vary depending on the complexity of the request. Requests must demonstrate a legitimate business purpose and must be relevant to the academic or administrative responsibilities of the sponsoring department or organization. All student data are released to and for use by the requesting department only. Authorized individuals and their designees (including contracted vendors) must agree to use the data provided only for the purpose specified in the request and, unless required and authorized, must agree that data obtained will not be reproduced, published, publicly posted, or used for any secondary purpose. Per IS-3, Unit Information Security Leads must dispose of electronic media containing Institutional Information classified at Protection Level 2 or higher, including damaged media and non-removable memory, in compliance with the UC Data Destruction Standard provided in BFB-RMP-2: Records Retention and Disposition: Principles, Processes, and Guidelines.

2. Misuse of student data may subject requestors or their designees to civil or criminal penalties and/or University discipline. To ensure compliance, all elements of the intended data uses must be stipulated in the request.

3. Email addresses for students are generally not provided to any departments, units, or organizations for the purpose of sending mass emails to students; refer to the Guidelines on Use of Mass Communications (Email) Services for additional information.

4. Requests for student data using either self-reported ethnicity, gender identity, or sexual orientation as a selection criteria are approved or denied in accordance with FERPA and only to campus officials demonstrating legitimate educational interest in those data. Such data may only be disclosed in the aggregate for reporting purposes when the data value is greater than 5.

5. The UC Merced Institutional Research and Decision Support (IRDS) department and the Office of the Registrar, with assistance from University Counsel as needed, enforce the Family Educational Rights and Privacy Act (FERPA), The Solomon Amendment, the UC Merced Principles Guiding the Use of Electronic Communications, UC BUS-43 (Appendix DS) - Data Security and Privacy, and the UC Electronic Communications policy.

B. Access Privileges

The authorization process and type of student data that may be provided vary according to the academic or administrative responsibilities of the sponsoring department. Campus personnel with access to student records data in any location or format should familiarize themselves with Family Educational Rights and Privacy Acts (FERPA). Requests for student data are evaluated and approved under the following guidelines:

1. **Academic Unit*:*** Student data may be provided to campus officials who demonstrate a legitimate business purpose.

2. **Administrative Unit*:*** Student data may be provided to other official University units at UC Merced or other UC campuses. This includes UC Merced business

entities. Requests must be authorized by the director or administrative manager of the unit and demonstrate a legitimate business purpose for requesting the data.

3. **Research Purposes:**

   a. Student data may be provided to researchers, Academic Senate Committees or their representatives who are affiliated with UC Merced and demonstrate a legitimate business purpose for requesting the data. The requestor must submit proof of UC Merced Institutional Review Board (IRB) approval or waiver when making a request for student data to be used in scholarly or campus research, including requests for email, addresses or phone numbers. However, disclosure of student data is an independent institutional prerogative and IRB approval has no bearing on the decision of the Registrar as to the appropriateness and approval of the data request. The request must also be authorized by the committee, dean, chair, or department head of the sponsoring UC Merced department. For student researchers, authorization by the researcher's faculty advisor at UC Merced is also required.

   b. In evaluating requests from researchers who wish to conduct research using student data, IRDS and the Office of the Registrar work cooperatively with the Campus Working Group on Assessment (CWGA), the Institutional Review Board (IRB), and other campus offices. The Office of the Registrar and/or IRDS may modify, approve, or deny requests from researchers based on recommendations from these groups. If the research involves surveying, IRDS and the Office of the Registrar work with other campus offices to determine the institutional impact of surveying students. For more information, see Survey Coordination at UC Merced. Requests for census sampling (i.e. surveying every person in a group) are generally not approved. In order to facilitate timely review of requests, proposals should include the desired sample size and justification for such based on the research design.

   c. The use of UC contracted/approved third-party applications (e.g., Qualtrics) to host a survey are acceptable, but the development of the survey must be done with careful attention to ensure student record information is not collected or maintained by non-contracted vendors. Student record information that is stored by a contracted vendor must only be accessible by individuals with a legitimate educational interest. Refer to Section 5 below for information about contracting vendors.

4. **Student Organizations:** Individuals requesting student contact data for UC Merced student organizations that are registered with the Office of Student Life (OSL) will be referred to the Guidelines on Use of Mass Communications (Email) Services and to the use of UC Merced Happenings messages.

5. **Third-Party/Vendor Organizations:** When a UC Merced department or organization makes plans to utilize a non-UC Merced entity (e.g., third-party organization or vendor) with a service or support effort that involves student records, the UC Merced department or organization and non-UC Merced entity must receive authorization from IRDS and the Office of the Registrar to host or collect student information.

All Third-party suppliers with whom the University of California contracts for services or resources that connect to UC information resources must agree to the UC Appendix - Data Security and Privacy, which is negotiated between Procurement and the vendor. UC Merced IT can provide a list of approved third party suppliers.

6. **The Public**

    a. Student data are not provided to the public, including individuals, businesses, and organizations. The public may obtain contact information for a specific set of students as allowed by FERPA using the UC Merced Directory.

    b. UC Merced has authorized National Student Clearinghouse to act as its agent for all verifications of student enrollment and degrees.

    c. Degree verification for the most recent term is available approximately eight weeks after the term ends.

    d. The media, including campus publications, must contact University Communications at communications@ucmerced.edu for all inquiries.

    e. The UC Merced Office of the Registrar provides student contact data to United States military recruiters under the guidelines of The Solomon Amendment.

    f. Requests under the Public Records Act should be sent to publicrecords@ucmerced.edu.

7. **Aggregate Data:** Aggregate data are not generally provided to any other requestor. Public institutional data is available at the IRDS web site at ipa.ucmerced.edu or the University of California web site at the University of California Information Center.

8. **Mass Email:** Individuals requesting student contact data in order to send mass email will be referred to the Guidelines on Use of Mass Communications (Email) Services and to the use of approved methods for broadcast messages and other strategies for contacting students, faculty and other affinity groups.

V. PROCEDURES

Requests for Student Data Access should be submitted at the Office of the Registrar website: registrar.ucmerced.edu/form/data-request.

VI. RESPONSIBILITIES (if applicable or necessary)

A. Unit Head Responsibilities

1. Unit Head or their named designee must:

a. Designate one or more people as the individual(s) responsible for overseeing the execution of information security responsibilities within the Unit.
b. Identify and inventory Institutional Information and IT Resources managed by the Unit.
c. Ensure Risk Assessments are complete and Risk Treatment Plans are implemented.
d. Inform service providers who manage IT Resources on behalf of the Unit of the Protection Level and Availability Level.
e. Through the risk management process, ensure that Institutional Information and IT Resources managed by service providers meet the requirements of this policy.
f. Through the risk management process, ensure that Institutional Information and IT Resources managed by suppliers meet the requirements of this policy.
g. Report to the Chief Information Security Officer (CISO) any security incidents.
h. Report to the CISO any information security policy or standard that is not fully met by the unit, or by a service provider managing institutional information or IT resources on behalf of the unit.
i. Ensure the above responsibilities are included in the overall Unit planning and budgeting process.

2. Unit Heads may delegate specific information security responsibilities to Workforce Members under their area of responsibility, Service Providers, or Suppliers. The Unit Head must ensure this delegation of responsibility is clear and unambiguous. Any unit information security responsibilities not expressly delegated to, and accepted by, a service provider or supplier remain the responsibility of the Unit Head.

B. Institutional Information Proprietor Responsibilities

1. Institutional Information Proprietors must:

a. Classify institutional information under their area of responsibility in accordance with this policy.
b. Establish and document rules for use of, access to, approval for use, and removal of access to the Institutional Information related to their area of responsibility.
c. Notify units, users, service providers, and suppliers of the institutional information protection level.
d. Approve institutional information transfers and access related to their responsibility.
e. Notify units, service providers, and suppliers of applicable records retention requirements.

VII. POLICY OR PROCEDURE REVISION HISTORY

Date	Action / Summary of Changes
August 8, 2017	Original Policy Issued
October 13, 2017	Technical Update (Appendix 1)

APPENDICES

APPENDIX 1 – UC Merced Release of Student Data

UC MERCED RELEASE OF STUDENT DATA

Last Updated October 13, 2017

CLASSIFICATION	GENERAL RELEASE/ACCESS GUIDELINES
DIRECTORY	Directory information may be disclosed unless the student files a nondisclosure.
INTERNAL	Release of information that requires the student's written permission.
PROTECTED	Campus officials with legitimate educational interest have access to student data subject to data security requirements. For information about legitimate educational interest, go to registrar.ucmerced.edu/policies/ferpa
SENSITIVE	Campus officials with legitimate educational interest have access to student data subject to data security requirements. Special circumstances may allow disclosure of aggregate data for reporting purposes. Otherwise, student's written permission is required for release with the exception of compliance with a judicial order or lawfully issued subpoena in consultation with campus Counsel.

Student Data for Release/Access	Groups Requesting Release/Access						
	UCM Student	Family/Guardian	General Public	UCM Student Club/ Organizations or Advisor	Education Agencies	UCM Staff/Faculty/ Departments	Gov't/Law Agencies or UCM Campus Police
Student Name							
Telephone, Email							
Major Field of Study							
Class Level (Year in School)							
Dates of Attendance			DIRECTORY				
Enrollment Status (Full Time/Part Time)							
Degrees & Awards Received							
Participation in Officially Recognized Activities							
Photographs							
Address							
Class Schedule							
Grade Point Average							
Course Grades							
Current or Completed Units							
Transcript							
Residency Status		INTERNAL				PROTECTED	SENSITIVE
Student ID Number							
Parent or Guardian Name/Address							
Social Security Number							
Ethnicity							
Gender at Birth							
Disability							
Gender Identity and Sexual Orientation		SENSITIVE					

NOTE: Information not listed above falls into either Classification Internal, Protected or Sensitive. The Office of the Registrar will consider the need for and intended use of the data in the decision to release it. The Data Operations and Stewardship Council will consider appeals to decisions.

UC Students' rights under the Family Educational Rights and Privacy Act (FERPA) begin as soon as they enroll or register with an academic program of the University. See http://registrar.ucmerced.edu/policies/ferpa for student rights under FERPA.