

NUMBER: ACAF 7.02
SECTION: Academic Affairs
SUBJECT: Data Access
DATE: February 1, 1995
REVISED: March 3, 2004
Policy for: All Campuses
Procedure for: All Campuses
Authorized by: Jerome D. Odom
Issued by: Provost's Office

1. Policy

Information maintained by the University is a vital asset that will be available to all employees who have a legitimate need for it, consistent with the University's responsibility to preserve and protect such information by all appropriate means. The University is the owner of all administrative data; individual units or departments may have stewardship responsibilities for portions of that data. The University intends that the volume of freely accessible data be as great as possible. While recognizing the University's responsibility toward the security of data, the procedures established to protect the data must not unduly interfere with the efficient conduct of University business. Unjustified barriers to accessing computerized institutional data must be avoided.

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its access. The University expressly forbids the use of administrative data for anything but the conduct of University business. Employees accessing data must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in any use.

The University determines levels of access to administrative data according to principles drawn from various sources. State and federal law provides clear description of some types of information to which access must be restricted. In an academic community, ethical considerations are another important factor in determining access to administrative data. This policy is for the internal use of information for employees at the University of South Carolina. External requests for information are handled in accordance with University Policy HR 1.00 "Freedom of Information Policy."

2. Definition of Administrative Data

The University's database consists of information critical to the success of the University as a whole. The University database is shared data, managed within a conceptual framework. It is likely that the University database will be distributed across processing units within the University.

Data may be stored on paper or as digital text, graphics, images, sound, or video. The University regards data that are maintained in support of a functional unit's operation as part of the University's administrative database to be official data if they meet any of the following criteria:

- if at least two administrative operations of the University use the data and consider the data essential;
- if integration of related information requires the data;
- if the University must ensure the integrity of the data to comply with legal and administrative requirements for supporting statistical and historical information externally;
- if a broad cross section of users refers to or maintains the data; or
- if the University needs the data to plan.

Some examples of administrative data include student course grades, employee salary information, vendor payments, and the University's annual Fact Book. Administrative data do not include personal electronic calendar information and similar material.

Copies of official data are NOT official data where they are found on diskettes, individual hard drives, network servers, or as files on other shared systems. These copies or downloads cannot be used as substitutes for official records kept by the authorized data stewards of the University. However, such information may be used to generate official reports on behalf of the University with the knowledge and permission of the data stewards. Such files and any resulting reports are covered by the same constraints of confidentiality and privacy as the official records.

Prior to the development of a system that will download official records and manipulate them for subsequent update or application to official records, permission must be obtained from the data steward for such transfer.

3. Data Trustees, Data Stewards and Data Users

Data Trustees are senior management personnel (typically at the level of Vice President, Associate or Vice Provost, Dean, or University Director) who have planning and policy-making responsibilities for data in their operational area. The Data Trustees, as a group, are responsible for overseeing the establishment of data management policies and procedures.

Data Stewards are managers of functional areas (typically at the level of Controller, Registrar, Director of Admissions or Director of Administrative Information Services) who oversee the capture, maintenance, and dissemination of data for a particular operation. Data Stewards are responsible for making security decisions regarding access to the data under their charge. Data

Steward responsibilities include the data management activities outlined in this policy and other activities that may be delegated by a Data Trustee.

Data Users are individuals who access University data in order to perform their assigned duties or to fulfill their role in the University community. Data Users are responsible for protecting their access privileges and for proper use of the University data they access (see Responsibilities of Users).

4. Responsibilities of Data Trustees, Data Stewards, and Computer Services

4.1 Categorization of Data

Data Trustees will assign each item of administrative data and each standard view of that data to one of three categories: general access, limited-access, or restricted.

4.1.1 General Access Data

General access data are all data that are not either restricted or judged by Data Trustees to be limited-access data. The accessible data volume should be as great as possible to enable those who need the information to have access. Data should be part of an open atmosphere and broadly available.

General Access data are subject to disclosure to all USC employees as well as the general public under the Freedom of Information Act.

4.1.2 Limited Access Data

Limited access data are data that the Data Trustees judge to require special procedures for access. Limited access data may be subject to disclosure under the Freedom of Information Act. Limited access data are made available to a select group of USC employees based on their job function.

4.1.3 Restricted Data

Restricted data are those data found upon review by the Data Trustees or General Counsel to require restrictions on access. Restricted data may not be subject to disclosure under the Freedom of Information Act. Restricted data are only available to USC employees that have a business or educational need to access the data.

4.1.4 Criteria for Determining Access

Data Stewards are ultimately responsible for assigning access to all types of data on an individual basis; however, general criteria for determining access to both restricted and limited access data include the following:

HR/Payroll data can be made available as follows:

- Personnel in the employee's supervisory chain of authority
- Human Resources/Payroll/Business contacts in departments and on Senior and Regional campuses will have access to HR/Payroll data for employees in their departments or campuses in the case of Senior and regional campuses.
- Authorized employees of the Division of Human Resources, Payroll, Department, Budget Office, Controller's Office, Cost and Contract Grant Accounting, Internal Audit, the Legal Office, the Office of Equal Opportunity Programs, and the Department of Law Enforcement and Safety, will have access to Hr/Payroll data on a case by case basis as appropriate for them to perform their job responsibilities. Similarly, HR/Payroll data will be provided on a case by case basis in response to judicial orders or lawfully issued subpoenas.
- Legally authorized law enforcement personnel, authorized Federal or State agencies, members of duly appointed grievance committees, representatives of authorized accrediting organizations, and agencies processing claims made by the employee for worker's compensation, unemployment insurance or other employee benefits which will have case by case access to the portions of the official personnel files which are appropriate for their business.
- To appropriate parties in a health or safety emergency.
-

Financial data can be made available as follows:

- President, Vice Presidents, Chancellors, Deans, Department Heads and other Personnel with responsibility for the management and oversight of financial resources
- Business Managers and business office staff in departments and on Senior and Regional campuses
- Authorized employees of the Division of Business and Finance, Office of General Counsel, Division of Law Enforcement and Safety and the Office of Internal Audit who have a business need to access the data

Student data can be made available as follows:

- To school officials with legitimate educational interests;
{A school official is a person employed by the University in an administrative, supervisory, academic or research, or support staff position; a person or company with whom the University has contracted (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.}
- A **school official** has a **legitimate educational interest** if the official needs to review an educational record in order to fulfill his or her professional responsibility.
- To officials of other institutions in which the student seeks or intends to enroll provided that the student had previously requested a release of his/her record;
- To authorized representatives of the U.S. Department of Education, the Comptroller General of the United States, state education authorities, organizations conducting studies for or on behalf of the University, and accrediting organizations;
- In connection with a student's application for, or receipt of, financial aid;
- To comply with a judicial order or lawfully issued subpoena;

- To parents of dependent students as defined by the Internal Revenue Code, Section 152;
- To appropriate parties in a health or safety emergency;
- To the alleged victim of any crime of violence of the results of any disciplinary proceedings conducted by the University.

4.2 Definition of Data

The Data Trustees and Stewards will establish procedures for initial definition and change of data elements within their data entity.

Data Stewards will provide data descriptions for directories that will let data users know what shareable data are available, what the data mean, and how to access the data.

Data definitions will be:

- based on actual usage,
- made according to University standards,
- modified only through approved procedures, and
- reviewed on a timely basis and kept current.

4.3 Definition of Data Extracts and Data Views

The Data Trustees will work with Data Stewards and data users to define useful and meaningful schedules for creation of standard data extracts (data snapshots that are captured at a fixed point in time).

The Data Trustees will work with the Data Stewards to define standard views of administrative data, in order to aggregate data from multiple sources, to segment data into smaller and more manageable subsets, or to segregate data according to confidentiality or similar characteristics. A data view is a logical entity only, typically assembled from the most current data from their primary storage location at the time they are requested.

4.4 Development of Access Policies and Procedures

The term "access" means to read or view administrative data. Access does not include the ability to create or modify data. Creation and modification can only be done by the Data Steward, the Data Trustee, or their designate.

Each Data Steward will be individually responsible for establishing data access procedures that are unique to a specific information resource or set of data elements. These procedures will ease access and will ensure data security.

4.5 Promotion of Accurate Interpretation and Responsible Use

Data Trustees will develop policy to promote the accurate interpretation and responsible use of administrative data.

Data Stewards are responsible for making known the rules and conditions that could affect the accurate presentation of data. Persons who access data are responsible for the accurate presentation of that data.

Data Stewards will support users in the use and interpretation of administrative data, primarily through documentation, but also in the form of consulting services.

4.6 Maintenance of Data Integrity

The Data Stewards will determine the most reliable sources of data and regularly evaluate the quality of the data entity. They will determine responsibilities for data capture and maintenance to ensure data integrity.

The Data Stewards will identify gaps and redundancies in the data and, to the extent possible, will ensure that only needed versions of each data element exist. They will specify data control and protection requirements to be observed by data processors and users.

The Data Stewards will monitor the data for accuracy, integrity, and dependability, and where appropriate, will initiate action concerning these issues.

4.7 Determination of Security Requirements

The Data Trustees, in consultation with Computer Services, will determine security requirements for administrative data and will be responsible for monitoring and reviewing security implementation and authorized access.

4.8 Establishment of Archiving Procedures

The Data Trustees and Stewards will define the criteria for archiving the data to satisfy retention requirements.

4.9 Establishment of Disaster Recovery Procedures

Computer Services is ultimately responsible for defining and implementing policies and procedures to assure that data are backed up and recoverable. The Data Trustees will play an active role in assisting Computer Services in this responsibility.

With the Data Trustees' advice, Computer Services will develop a workable plan for resuming operations in the event of a disaster, including recovery of data and restoration of needed computer hardware and software.

4.10 Responsibilities of the Administrative Information Services

Administrative Information Services (AIS) develops and applies standards for the management of institutional data and for ensuring that data are accessible to those who need it.

AIS works with the Data Trustees to establish long-term direction for effectively using information resources to support University goals and objectives.

AIS creates logical data models of applications. These models are ultimately used to create an institution-wide data model that cross-references data across applications and encourages data sharing.

AIS develops a standard method for naming and defining data. It also facilitates conflict resolution in data definitions.

AIS makes institutional data available to authorized users in a manner consistent with established data access rules and decisions. It develops views of data as directed by the Data Trustees and Data Stewards. The group ensures that the technical integrity of the data is maintained and that data security requirements are met.

5. Requests for Access

5.1 Restricted or Limited-Access Data

Access to restricted or limited-access data by University employees or employees of University-related foundations requires that a formal request be made to the appropriate Data Steward.

5.2 Exceptions

All requests for exceptions to data access policies must be made in writing to the Data Steward. E-mail requests are acceptable. The request must specify the data desired and their intended use.

5.3 Denial

The Data Steward must provide a written record of the reasons for denial of any access request. E-mail records are acceptable.

6. Responsibilities of Users

6.1 Use of administrative data only in the conduct of University business

The University expressly forbids the disclosure of unpublished administrative data or the distribution of such data in any medium, except as required by an employee's job responsibilities and approved in advance by the Data Steward. In this context, disclosure means giving the data to persons not previously authorized to have access to it. The University also forbids the access or use of any administrative data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity. Users agree to use the information only as described in the request for data access.

6.2 Maintenance of confidentiality and privacy

Users will respect the confidentiality and privacy of individuals whose records they access, observe any ethical restrictions that apply to data to which they have access, and abide by applicable laws and policies with respect to access, use, or disclosure of information. All data

users having access to restricted or limited-access data will formally acknowledge (by signed statement or some other means) their understanding of the level of access provided and their responsibility to maintain the confidentiality of data they access. Each data user will be responsible for the consequences of any misuse. Users are expressly prohibited from releasing identifiable information to any third party.

6.3 Protection of data

Users will comply with all reasonable protection and control procedures for administrative data to which they have been granted access.

6.4 Accurate presentation of data

Users will be responsible for the accurate presentation of administrative data, and will be responsible for the consequences of any intentional misrepresentation of that data.

The Office of Institutional Planning and Assessment shall be the University's clearinghouse for official reports to external agencies including federal and state governments.

6.5 Management Oversight

All levels of management are responsible for ensuring that all data users within their area of accountability are aware of their responsibilities as defined in this policy. Specifically, managers are responsible for validating the access requirements of their staff according to their job functions, and for insuring a secure office environment. The head of each unit will authenticate the need for individual access to data and must request and obtain authorization for access to data from the steward of such data.

Administrative and academic unit heads are responsible for taking the necessary steps to ensure that data access is terminated for employees who transfer to another department within the University or leave employment of the University. [Please see University Policy ACAF 7.02.]

7. Appendix A – Data Trustees

University of South Carolina Data Trustees	
Payroll Data	Vice President and Chief Financial Officer
Financial Data	Vice President and Chief Financial Officer
Facilities Data	Vice President and Chief Financial Officer
Human Resources Data	Vice President for Human Resources
Library Data	Dean of Libraries
Development Data	Vice President for University Advancement
Admissions Data - Graduate, Law, Medicine	Executive Vice President for Academic Affairs and Provost
Admissions Data - Undergraduate	Vice President for Student Affairs
Alumni Data	Vice President for University Advancement
Financial Aid Data	Vice President for Student Affairs
Student Data	Executive Vice President for Academic Affairs and Provost
Student Medical Data Student Counseling Data Student Housing Data Student Discipline Data	Vice President for Student Affairs
Student Advisement Data	Executive Vice President for Academic Affairs and Provost
Course Data	Executive Vice President for Academic Affairs and Provost
Faculty Data	Executive Vice President for Academic Affairs and Provost
Communications Data	Vice President and Chief Financial Officer

8. Appendix B – Data Stewards

University of South Carolina Data Stewards	
Financial Data Payroll Data	Controller Director of Accounting Services Director of Financial Services/Bursar Budget Director Assistant to the Vice President for Business & Finance Director of Cost and Contract/Grant Accounting Director of Payroll Director of Purchasing Director of Health & Safety
Facilities Data	Director of Facilities Management & University Architect
Human Resources Data	Director of Salary Administration & HR Systems HRIS Manager
Library Data	Librarian for Administrative Services
Development Data	Senior Director, Advancement Administration Senior Director, Advancement Services
Admissions Data	Director , Undergraduate Admissions Director, Graduate Admissions Assistant Dean of Admissions, Law School Director of Enrollment Services and Registrar, School of Medicine Directors of Admissions, Senior and Regional Campuses
Alumni Data	Senior Director, Advancement Administration Senior Director, Advancement Services
Financial Aid Data	Director, Student Financial Aid and Scholarships Regional Financial Aid Officers

University of South Carolina Data Stewards	
Student Data	University Registrar Senior Associate Registrar Director of Financial Services/Bursar Director of Housing and Judicial Programs Director, Student Health Services Director, Counseling and Human Development Centers University Archivist Associate/Assistant Deans/Student Services Coordinators Department Chairs Director, Graduate Admissions
Course Data	University Registrar Senior Associate Registrar
Faculty Instruction Data	University Registrar Senior Associate Registrar
Communications Data	Director of University Information Systems

9. Appendix C - Itemization of University Data

9.1 General Access

9.1.1 Data Available from University of South Carolina Fact Book

General Information

- History of the University of South Carolina
- The University Perspective
- Mission Statement
- Accreditations
- Board of Trustees
- Administrative Officers
-

University Enrollment

- Statistical Summary for the University
- Fall Enrollment
- Spring Enrollment
- Summer Enrollment
- Enrollment by Race
- Percentage of Enrollment by Race
- Enrollment by Full-Time/Part-Time and Gender
- Undergraduate Enrollment by Class
- Geographic Origin by Students by State

- Top Ten Enrollment by State
- Geographic Origin of Students by County
- Top Ten Enrollment by County
- Geographic Origin of Students from Foreign Countries
- Fall FTE Enrollment

Columbia Campus

- USC Columbia Mission Statement
- Statistical Summary for Columbia
- Student Data
 - Fall Enrollment (Majors)
 - Spring Enrollment (Majors)
 - Summer Enrollment (Majors)
 - Enrollment (Majors) by Race
 - Enrollment (Majors) by Gender
 - Enrollment by Gender
 - Enrollment (Majors) by Full-Time/Part-Time
 - Full-Time/Part-Time Enrollment
 - Enrollment (Majors) by Classification
 - Age Distribution by Majors
 - Fall FTE by College
 - Fall FTE Percentage Distribution by College
 - New Freshman Profile
 - New Freshmen and New Transfer Applications
 - Graduation Rate (%) as of Fall 1997
- Degree Information
 - Degrees Awarded by Profile
 - Degrees Awarded by Program
 - Degrees Awarded by School and College
- Financial Information
 - Sponsored Programs & Research - By Purpose
 - Sponsored Programs & Research - By Source
 - Current Funds Revenue and Expenditures - Columbia
 - Current Funds Revenue and Expenditures - School of Medicine
- Faculty Data
 - Age Distribution of Full-Time Ranked Faculty
 - Full -Time Ranked Faculty by Highest Degree Received
 - Average Full-Time Teaching Faculty Salaries
 - Distribution of Full-Time Ranked Faculty

Four Year and Regional Campuses

- Statistical Summary for the Four Year and Regional Campuses
- History of Four Year and Regional Campuses
- Fall Enrollment by Gender
- Fall Enrollment by Race
- Spring Enrollment by Gender

- Spring Enrollment by Race
- Summer I Enrollment
- Summer II Enrollment
- Associate Degrees Conferred
- Geographic Origin of Students by State
- Geographic Origin of Students by County
- Geographic Origin of Students from Foreign Countries
- Current Funds Revenues and Expenditures
- Full-Time Ranked Faculty by Highest Degree Received
- Full-Time Ranked Faculty by Salary

9.1.2 Data Available from Financial Schedules

Financial Report - System, Regional Campuses, and Medical School

- Balance Sheet
- Statement of Changes in Fund Balances
- Statement of Current Funds Revenues, Expenditures, and Other Changes
- Notes to the Financial Statements

9.1.3 Data Available from Human Resources

- Employee Information:
 - Name
 - Campus Address/Phone: Department, Building, Room
 - E-mail address
 - Endowed Chairs
 - Gender
 - Race
 - Title (Class & Internal Title(s))
 - Date of Employment

9.1.4 Data Available from Student Records

- Name
- Electronic mail address
- Local mailing address and telephone number
- Permanent mailing address and telephone number
- Semesters of attendance
- Enrollment status (full- or part-time)
- Date of admission
- Date of graduation
- School, major and minor fields of study
- Whether or not currently enrolled
- Classification (freshman, etc.)
- Type of degree being pursued
- Degrees, honors and awards received (including scholarships and fellowships)

- Weight and height of members of athletic teams
- Whether the student has participated in officially recognized activities and sports sponsored by the University

NOTE: This information is not available to anyone who does not have an educational need to know (defined in section 4.1.4) if the student has completed a request for privacy as outlined in the Notification of Student Rights Under FERPA which is published in the University catalogs, the Master Schedule of Classes, and the Carolina Community.

9.2 Restricted and Limited Access

9.2.1 Human Resources/Payroll Data

Restricted	Limited Access
<ul style="list-style-type: none"> ▪ Medical ▪ Garnishments ▪ Benefits Personal Nature: <ul style="list-style-type: none"> ▪ Handicapped / disability status ▪ Home/Mailing Address ▪ Home Phone ▪ Date of Birth ▪ Social Security Number ▪ Marital Status 	Personal Nature: <ul style="list-style-type: none"> ▪ Education
<ul style="list-style-type: none"> ▪ Total Compensation 	<ul style="list-style-type: none"> ▪ Total Compensation (as defined under FOI)
Performance <ul style="list-style-type: none"> ▪ Review Rating ▪ Review Date ▪ Pay for Performance 	
<ul style="list-style-type: none"> ▪ Salary History/Employment History 	<ul style="list-style-type: none"> ▪ Salary History/Employment History (as defined under FOI)
Basic Information: <ul style="list-style-type: none"> ▪ Emergency Contact & Phone ▪ Leave Balances ▪ Training Records 	Basic Information: <ul style="list-style-type: none"> ▪ State Service Date ▪ Leave Base Date ▪ Class/Slot ▪ Exempt/Non-exempt status ▪ Salary Band

Restricted	Limited Access
<ul style="list-style-type: none"> ▪ Employee Disciplinary Records 	Basic Faculty Data: <ul style="list-style-type: none"> ▪ Tenure Status ▪ Tenure Date ▪ Tenure Department ▪ Date on Tenure Track ▪ Date of Rank ▪ CIP of Degree
<ul style="list-style-type: none"> ▪ E-mail files concerning or created by an employee 	<ul style="list-style-type: none"> ▪ Accounting Information/FTE
<ul style="list-style-type: none"> ▪ Employee ID Photographs 	<ul style="list-style-type: none"> ▪ Supervisor (Name, Class, Slot)

9.2.2 Student Data

Restricted	Limited Access
Personally identifiable student data not designated as Directory Information: <ul style="list-style-type: none"> ▪ Student identification (usually Social Security Number) ▪ Admissions data ▪ Financial aid data ▪ Student enrollment data, including student course schedule and grades ▪ Student accounts data ▪ Student disciplinary records ▪ Student employment records (if employment is contingent upon enrollment) ▪ E-mail files concerning or created by a student ▪ Student ID photograph ▪ Student medical and counseling data ▪ Student advisement data 	<ul style="list-style-type: none"> ▪ Faculty Instruction Data

9.2.3 Financial Data

Restricted	Limited Access
<ul style="list-style-type: none"> ▪ Donor Information (if donor requested that privacy be maintained) 	<ul style="list-style-type: none"> ▪ All financial data

Download the Appendix D as shown below - [Statement of User Responsibility in pdf.](#)

Employee Name - Printed (Last, First)

10. Appendix D – Statement of User Responsibility

I understand that by virtue of my employment with the University of South Carolina, I may have access to data, information, systems, or files in various forms which contain individually identifiable information, the disclosure of which may be prohibited by federal or state law or by University policy. I acknowledge that the intentional disclosure by me of this information to any person could subject me to criminal and civil penalties imposed by law. I further acknowledge that such willful or unauthorized disclosure may also violate University of South Carolina policy and could constitute just cause for disciplinary action including termination of my employment on the first offense regardless of whether criminal or civil penalties are imposed.

If I am in doubt about a request, I will consult with my supervisor prior to releasing the information.

My signature denotes that I have read and understand the above statement.

Signature of Employee

Date

Signature of Supervisor

Date