

## University Community (faculty, staff and students)

### **Privacy of Personal Information**

The University of Southern California is committed to the responsible use of personal information collected from and about students, faculty, staff, business partners and others who provide such information to us and to compliance with both state and federal regulations concerning the use of personal information. Such personal information includes any number that may be used, alone or in conjunction with any other information, to identify a specific individual; or other personal information that could be used to cause financial or reputational harm to an individual. This policy applies to information that is collected by any means whether electronically, by telephone, or on paper.

#### **Limits on Use and Access**

The responsible use of personal information requires that the university respect individual privacy, protect against identity theft and other unauthorized uses, and comply fully with all laws and government regulations in the collection, use, storage, display, distribution and disposal of such information. Authorized uses of personal information within the university are limited to those which a) are necessary to meet legal and regulatory requirements; b) facilitate access to services, transactions, facilities and information; or c) support efficient academic and administrative processes.

Access to personal information is limited to

- the individual whose information is produced or displayed,
- a University official or agent of the university with authorized access based upon a legitimate academic or business interest and a need to know,

---

Issued by: Dennis F. Dougherty  
Senior Vice President,  
Administration

Lloyd Armstrong, Jr.  
Provost and Senior Vice President,  
Academic Affairs

Date issued: December 1, 2004  
University of Southern California  
Page 1 of 4

- an organization or person authorized by the individual to receive the information,
- a legally authorized government entity or representative, or other circumstances in which the University is legally compelled to provide access to personal information, or
- other individuals or entities, as allowed by law, for purposes judged to be appropriate or necessary for the reasonable conduct of University business.

### **Social Security Numbers**

State law protects the use of Social Security numbers. The University will continue to collect and maintain Social Security numbers in all instances in which that number is required by law for reporting or other uses. This includes, but is not limited to, all enrolled students who are U.S. citizens or permanent residents, and all individuals receiving payment from the University. In addition, the University will continue to use Social Security numbers, as allowed by law, for operational purposes for which there is no reasonable substitute. Social Security numbers are always considered confidential, and therefore subject to the access restrictions described above.

It is against both state law and university policy to

- Publicly post or display the Social Security number in any manner;
- Print the Social Security number on any card required to access service;
- Require an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the number is encrypted;
- Require an individual to use his or her Social Security number to access an Internet site unless a unique password or PIN is also required; or
- Print a Social Security number on any materials that are mailed unless required by a state or federal agency, unless state or federal law requires the Social Security

---

Issued by: Dennis F. Dougherty  
Senior Vice President,  
Administration

Lloyd Armstrong, Jr.  
Provost and Senior Vice President,  
Academic Affairs

Date issued: December 1, 2004  
University of Southern California  
Page 2 of 4

number to be on the document to be mailed. Also, Social Security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the Social Security number.

### **Department and Personal Responsibility**

Each university department is responsible for reviewing and monitoring internal procedures, reports and other documents to assure compliance with this policy. This responsibility includes providing training and control systems for the responsible use of personal information that is accessible to employees for doing the work of the department. The University expects that all members of the community also will exercise caution in making available their own personal information to others. In particular, individuals should not give others access to their USC identification cards, passwords or personal identification number (PIN).

### **Online Collection of Personal Information**

University departments that collect personal information on their Web pages must post a link to this privacy policy and inform consumers about any persons or entities outside the university with whom they may share personal information collected online. If the department has a process for the consumer to change such information, that process must be described and available to the consumer on the department Web pages. Any changes to this privacy policy will be posted on the USC Web site.

### **Personal Biomedical Information**

Medical records, records pertaining to personal health information and records pertaining to human subjects in research projects are governed by more extensive restrictions. For more information concerning human subjects research, refer to <http://www.usc.edu/admin/provost/irb>.

---

Issued by: Dennis F. Dougherty  
Senior Vice President,  
Administration

Lloyd Armstrong, Jr.  
Provost and Senior Vice President,  
Academic Affairs

Date issued: December 1, 2004  
University of Southern California  
Page 3 of 4

## Information Requiring Enhanced Protection

In addition to this privacy policy, please refer to the university's Information Security Policy for additional security requirements for personal information and other types of information that require enhanced privacy protection.

## Resources

The following offices have responsibility for providing interpretation and implementation guidance on this policy. Questions about the policy should be directed as follows:

*Complaints about online collection of personal information or compliance with the California Online Privacy Protection Act*  
Office of Information Security (213) 743-4900

*For issues or complaints regarding use or misuse of your own personal identification information*  
Students – Dean of Academic Records and Registrar (213) 740-4623  
Faculty – Vice Provost for Faculty Affairs (213) 740-6715  
Staff – Director, Personnel Services (213) 740-7953

*System Access, Security and Access Termination*  
Administrative Information Services (AIS) (213) 821-2000  
Information Services Division (ISD) (213) 740-5555

*Vendor/Contractor Access to Information and Confidentiality Agreements*  
Disbursement Control (213) 740-2720  
Purchasing Department (213) 740-2281

*E-Mail and Internet, Intranet, Extranet Uses of Personal Information and Disposal of Electronic Records and Computers*  
Office of Information Security (213) 743-4900

---

Issued by: Dennis F. Dougherty  
Senior Vice President,  
Administration

Lloyd Armstrong, Jr.  
Provost and Senior Vice President,  
Academic Affairs

Date issued: December 1, 2004  
University of Southern California  
Page 4 of 4