

## Pitzer College User Agreement and Data Security Policy

The use of technology to store, transmit, and manipulate information has greatly increased the productivity of staff at Pitzer College. Its use also brings increased data integrity and security concerns related to Administrative Information.

*Administrative Information* is defined as any data related to the business functions of the College and there are several levels listed below. This includes, but is not limited to financial, personnel, student, alumni, donor, and communications records. It does not include *Academic Information* such as library holdings and instructional notes.

- *Public information* is either faculty-staff directory information or that which is disseminated by the Office of Public Relations. Request for non-directory public information must be referred to that office. Without authorization, you should assume only that name, title, office phone number, and email address are public information for faculty and staff. Since students may elect to have their directory information reclassified to confidential, requests for information about students must be referred to the Registrar's Office. Requests for information on members of any other constituency should be referred to the Advancement Office.
- *Internal information* is that which, though widely disseminated throughout the College, is not generally available outside of the College. Examples include course schedules and resource inventories.
- *Sensitive information* is that which, if disclosed to unauthorized parties, altered, or destroyed, could result in significant inconvenience or loss of staff time, productivity or do harm to the Pitzer reputation. All output from administrative databases should be considered to be *sensitive* unless otherwise categorized.
- *Confidential information* is that which the College is required by law to keep private or which would adversely impact the ability of the College to perform its mission were it disclosed to unauthorized parties, altered, or destroyed. All aspects of personnel and development records are considered confidential, as are all aspects of student records, except for those defined as "directory information."

Securing data:

- *Physical security* should be employed when possible to reduce risk. This means using door and file drawer locks to keep unauthorized persons from viewing computer monitor screens and paper output or gaining access to magnetic media or user sessions connected to servers.
- *Passwords* are used to prevent unauthorized access to desktops and laptops as well as networked volumes and databases. Users are responsible for following the password guidelines for each system they access. This includes using a

password protected screen saver on desktops and laptops. All passwords should be kept secure at all times.

- *Firewalls* are setup by Information Technology staff to keep unauthorized users away from internal resources. Crossing a firewall may require the use of a Virtual Private Network. More information is available by contacting Help@pitzer.edu
- Viruses and worms are rampant on the Internet and all networked computers should be inoculated with the latest *anti-virus software* and maintained with the latest *system and application updates*. Contact the Computing Help Desk for assistance.
- Users are responsible for ensuring that all of their data are *backed up*. Backups of networked volumes are the most dependable and are done automatically by Information Technology. Because of this, users should store their data on networked volumes whenever possible. For special situations and for help with backups, contact the Help Desk.

Employees agree to inform their supervisors of any hindrances to good data management practices and to work to eliminate them.

Employees, including student employees, are granted access to institutional data only so they may conduct College business. They must respect the confidentiality and privacy of individuals whose records they access and abide by applicable laws or policies with respect to access, use, or disclosure of information. They may not disclose data to others (except as required by their job responsibilities), use data for their personal gain or for the profit of others, or access data to satisfy their personal curiosity. At all times they must maintain the integrity and security of administrative information. Employees who violate this policy are subject to the investigative and disciplinary procedures of the College--up to and including termination.

I understand that I am responsible for the security of all data I generate or use and have read this document and agree to abide by its provisions.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Department