

Confidentiality of Student and Employee Data

I. Regulatory and policy requirements governing access and use of information

It is the responsibility of those who use student and/or employee data maintained by the University as part of their normal job responsibility to understand the policies governing the use of that data. Regarding student data, both federal and California state laws govern access to and use of student information. Most student information maintained by the University is considered confidential under the Family Educational Right to Privacy Act (FERPA), the Privacy Act of 1974, and the California Information Practices Act. This would include personal information as well as course schedules, SSNs, and the Fresno State ID. The Privacy Act and the Information Practices Act also protect personal information about employees and independent contractors.

II. What is confidential?

Users of our campus student and employee data base should consider all information confidential.

The following directory information about students may be disclosed **ONLY** by Student Affairs and the Registrar's Office to third parties unless a student places a restriction on the release of directory information:

- a. name
- b. major
- c. participation in officially recognized university sports and student activities
- d. weight and height of members of athletics teams (disclosed by Athletics)
- e. enrollment status (undergrad, grad, full-time, part-time)
- f. transcript notations of degrees, awards, honors (including dates received) at Fresno State
- g. most recent educational institution attended

The release of additional information would require written permission from the student, a health and safety emergency, or a valid subpoena prior to releasing the information to a third party.

Faculty and staff are not authorized to release any of the above information to third parties.

Similar caution should be exercised when using employee information all of which is considered confidential except a-f below which is readily available to the public. The following employee information is considered public information and is generally accessible through campus directories or other public documents:

- a. name
- b. title or position
- c. classification
- d. salary
- e. campus phone
- f. campus office address

Release of confidential information or use of information other than for the conduct of university business is a violation of governing laws and campus policy. It is expected that faculty may need access to confidential information to adequately advise their students. This is an appropriate use of the data maintained by the university.

III. What is a "secure location?"

Information obtained in the normal course of one's job is to be kept in a secure location. Secure locations would include locked files (physically or electronically locked) as well as electronic devices which are not normally accessible to the public or others without authorized access. For example, keeping grades on a laptop or desktop computer issued to a specific individual, that is normally secured in that individual's office or regular off-campus work area, is an acceptable secure location. Keeping confidential information on external disks in areas easily accessed by unauthorized individuals is not acceptable. Discussion of confidential information in a public or non-business location where the conversation could be overheard by others would be considered a violation of the confidentiality of the data. Examples of placing confidential information in unsecured locations include:

- a. posting grades on an office door with either the SSN (or any portion of it), name, or Fresno State ID number (or any portion of it)
- b. discussing someone's disability in front of others
- c. distributing a report containing SSNs or Fresno State ID numbers beyond those with a business need for the report

If you have any questions about specific data or types of use, contact Student Affairs, Academic Personnel, or Human Resources.