

ANGELO STATE UNIVERSITY

**Federal Family Educational Rights and Privacy Act (FERPA)
COMPLIANCE STATEMENT**

The Federal Family Educational Rights and Privacy Act (FERPA) and the University's Faculty Staff Handbook (Chapter V, Section 20) govern the conduct of University employees with access to student records. To ensure compliance, the University requires that employees be aware of Federal law as well as System and University regulations that govern student records. This statement clarifies the responsibilities of persons with access to student educational records. **Note:** Staff in the Admissions Office, Financial Aid Office, Student Bursar's Office, Graduate Studies Office, and Registrar's Office sign this agreement as a condition of employment; others sign this statement as a condition of gaining access to the student records systems.

Confidentiality. Security passwords must remain confidential. Employees must log off the Banner student system when leaving their computer workstation.

Education Records. Employees may access Banner student records only as required to perform assigned duties. They may not update their own record or that of a friend or relative. Within the University, anyone whose designated responsibility requires access may use information from student records for appropriate research, educational, or service functions.

To respond to an inquiry from outside the University, verify whether the student has checked the "Confidentiality" box" on his/her records. This designation can be found on SPAPERS. Release of information regarding a group of students, such as a request for all seniors' mailing addresses, must be handled through the Student Life Office in coordination with the Registrar's Office. Unless explicitly suppressed by the student, the following "public" information may be released:

Student's name, local and permanent mailing address, e-mail address(es), telephone number(s), date and place of birth, photograph, marital status, major and minor fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, team photographs, dates of attendance, enrollment status, classification, degrees, awards and honors received, previous educational agencies or institutions attended, hometown, parents' names and mailing addresses.

All other information is private and may be released outside the University only with the student's written permission. No information, public or private, on an applicant's record may be released outside the University, except to an agent designated by the applicant, until the applicant becomes a registered student and has a chance to initiate a suppress. No information on financial aid records may be released outside the University except as authorized or required by federal and state regulations. **Also, within the University, publishing of non-directory information, especially social security numbers and campus ID's, should be kept to an absolute minimum. (Publishing includes, but is not limited to, copies of the information for office or workgroup use, formal reports, and fact books.) Such publishing should be limited to within office or workgroup use. Identification numbers should never be**

published in documents intended for general consumption. Hard-copy documents should be kept in secured locations, and electronic files should not be kept on laptop hard-drives.

Staff granted access to Banner student institutional databases or batch files agree to:

- Comply with all data standards policies as presented in the Guidelines for Data Standards, Data Integrity and Security ;
- Store information under secure conditions;
- Make every effort to ensure students' privacy;
- Destroy information when it is no longer needed;
- Use information only as described in the request for data or access to institutional database files;
- Release information to a third party only if authorized approval is given;
- Never represent summary data from files as "official" University data.

Violations. Violation of Federal law, System policy, or University policy constitutes grounds for rescinding access to Banner records or imposing disciplinary action, up to and including dismissal. Violations include the following offenses and any other comparable action:

- Not adhering to data standards guidelines as presented in the Guidelines for Data Standards, Data Integrity and Security
- Releasing public information about student requested on the basis of non-public information (e.g., names of all international students, name of all students with a GPA lower than 2.0);
- Altering a student's record without appropriate supporting documentation/authorization, regardless of whether you benefit from this alteration;
- Accessing a student record outside of your assigned duties;
- Releasing suppressed or private information without authorization;
- Publicly discussing a student's record in a way that might personally identify that student;
- Sharing computer security passwords.