



ANGELO STATE UNIVERSITY

Request for Access to Banner/Student Information: Dual Credit

DUAL CREDIT USE ONLY:

This form is for Dual Credit Instructors or Counselors to receive access to RamPort (part of the Banner System), or for Dual Credit Proctors to receive access to view their students' progress in online courses in Blackboard. Return this form to the Dual Credit Office: dualcredit@angelo.edu or fax to 325-942-2078.

Section 1 - USER INFORMATION

Instructions:

1) Fill in yellow highlighted sections. Print the form. 2) Read & sign Section 2. 3) Return form to the Dual Credit Office.

Name: Last First MI Date

Campus ID# Title Adjunct Instructor/Counselor/Proctor Department Dual Credit Program

All users MUST have an ASU Technology Access Account (TAA) before being granted access to Banner or Banner Self Service (through RamPort).

ASU Username (i.e., ASMITH)

ASU Username input box

- Type of Access: New Account, Revised Access, Delete Access
Status: Staff, Faculty, Student, Other
Type of Position: Permanent, Part-Time/Hourly, Temporary (e.g., Dual Credit Instructor/Proctor, Temps, students)

Section 2 - COMPLIANCE

Federal Family Educational Rights and Privacy Act (FERPA). The Federal Family Educational Rights and Privacy Act (FERPA), the Texas Tech University System Rules and Regulations, and/or the University's Faculty/Staff Handbook govern the conduct of employees and School Officials (as defined below) with access to student records who act in the student's educational interest within the limits of the employee's or School Official's need to know.

A School Official is a person employed by the University in an administrative, supervisory, academic or research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the University has contracted as its agent to provide a service instead of using University employees or officials (such as an attorney, auditor, collection agent, or dual credit instructor/proctor); 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.

Confidentiality. Your security password should remain confidential. You must log off the Banner student system when leaving your computer workstation or otherwise secure your system from misuse.

Education Records. You may access Banner student records only as required to perform assigned duties. You may not update your 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, you must check whether the student has checked the "Confidentiality" box on his/her records. This 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 by the designated Officer of Public Records in coordination with the Registrar's Office. Unless explicitly suppressed by the student, the following "public" directory information may be released:

- Student's name, local and permanent mailing address, ASU 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.

(Continued on Page 2)

Please sign on Page 2

Section 2 -COMPLIANCE (continued)

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 factbooks.) 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 data base 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.

_____ I have read this compliance statement and agree to the conditions and terms outlined herein.

Signature of User

For Head Data Custodian Use Only	Date Copied and Sent to IT _____	Approved for Cross Access _____	Initials _____
For IT Use Only	Date Completed _____	Initials _____	Last Revised 10/7/2019
