Protection of Student Records

The Office of the Registrar ensures the security of student records by:

- Securing files in the Student Records Vault and limiting access to authorized personnel only
- Restricting access to electronic student records information to those needing it to perform essential job functions
- Locking spaces where records and student information are used and stored
- Limiting the display of social security numbers to only those needing it to perform essential job functions
- Limiting access to work spaces to authorized personnel
- Requiring everyone, including student workers, to sign confidentiality agreements
- Requiring students, and others as needed, to present a photo ID for identification purposes before releasing non-directory information
- Utilizing screen protectors on computer monitors to keep unauthorized personnel from viewing student information during normal business hours
- Utilizing password-protected workstations to keep unauthorized personnel from logging on to staff computers after hours

Other University offices and departments implement procedures as recommended or used by the Office of the University Registrar to ensure security of student records campus-wide including:

- Using password protected databases
- Limiting access to passwords
- Locking file cabinets and drawers with student records
- Locking offices where records are used and stored
- Shredding appropriate documents as needed or required

Access to the student information database is restricted to individuals with a legitimate need to know or who must have access to student information in order to perform required job functions. A careful analysis is performed on all access requests by the appointed data manager. Administrative user access to the Banner Student database is restricted to the smallest number of users possible. Access is only granted after the request is reviewed and approved by the Registrar, the data manager for the Banner Student module. When needed, the Registrar works with departments and other administrators to clarify requests before a decision is made. If the access request is approved, IT Services creates an account for the user. Each year, a review by supervisors is required to reauthorize those employees who should maintain their access to Banner Student data. Employees granted access to student data must sign an agreement stating that they understand the statutes protecting the data and will uphold them.
For more information, see Administrative Policy # 74