Security Policy for Administrative System Users (Banner Data)

All employees of Winthrop University (administrative, academic, staff and student workers) are required to abide by the policies governing review and release of student education records. The Family Educational Rights and Privacy Act (FERPA) of 1974 mandates that information contained in a student's education record must be kept confidential and outlines the procedures for review, release and access of such information. Likewise, all employees are required to protect the privacy of all personal information for employees or students; including names, addresses, phone numbers (either home or work), Social Security numbers, etc.

Access to Banner data will be granted to those individuals who have been determined to have a legitimate educational or work related interest in the data. Access to specific data will be granted by approval of the Director of the functional area which oversees the data being requested.

Individuals who have been granted access to Banner data must understand and accept the responsibility of working with confidential student and employee records. The following rules apply to all University employees with a Banner account:

1. Every employee given access to the system will be given a username (or number) and password. Passwords are to be kept confidential and should not be shared or given to anyone, including supervisors, co-workers, student employees, or friends.

2. In all transactions, employees shall use their own username (or number). When authority to access additional screens or systems is needed, employees should make a request through their departmental supervisor to the appropriate security officer. Each employee given access is held responsible for any data which are input or retrieved using that username. All transactions on the system can be traced back to the username which was utilized to access the data.

3. It is the responsibility of each employee to keep his/her password confidential and to change passwords whenever they feel someone else may have obtained access to it.

Regarding personal or financial information for employees, or employees who may also be students, it is the practice of Winthrop University that personal or financial information of any kind is not provided to anyone, including other Winthrop employees, unless there is a bona fide business need. Requests for personal employee information should be referred to the Office of Human Resources; and requests for financial employee information should be referred to the Controller's Office. These departments will determine when there is a bona fide business need. When the "confidential" flag is indicated on the employee or student record in Banner, there may be extenuating circumstances that could threaten the employee's or student's safety in the event that personal or financial information about that employee or student is disclosed.

A complete policy statement on the Winthrop implementation of FERPA guidelines can be found on the Office of Records and Registration's website. In part, the policy states that officials of the University may be given access to student education records on a "need-to-know" basis and that such access must be limited to job-related, legitimate educational interests. The information contained in a student's education record may not be released to a third party without the written consent of the student. The only exception would be directory information defined as student name, address, e-mail address, telephone number, date and place of birth, enrollment status (full- or part-time), dates of attendance, date of graduation, major and minor fields of study, degrees and awards received, date of admission, whether or not currently enrolled, classification (freshman, etc.), most recent previous educational institution attended, eligibility for honor societies, participation in officially recognized activities and sports, weight and height of members of athletic teams and photographic, video or electronic images of students taken and maintained by the university. However, the preceding information may not be released for any students who have elected record privacy as indicated by the confidentiality flag.

Inappropriate use or misuse of student records is a violation of South Carolina and federal statutes and could result in civil and/or criminal prosecution. Inappropriate use or misuse of an employee's personal information or protected health information may be in violation of state or federal privacy laws.

_____ Employee Initials

_____ Campus ID (ex. W12345678)

Examples of inappropriate use of Banner data are:

1. Accessing or reviewing data without a legitimate educational interest, or a bona fide business related need.

2. Releasing confidential student information (non-directory) to another student, University organization, any person who does not have a legitimate educational interest, or parents of a dependent student, without the student's written authorization. Agencies requesting listings of majors for employment recruiting does NOT qualify as “need to know”.

3. Releasing confidential personal or financial employee information to anyone without a pre-approved bona fide business need.

4. Leaving reports or computer screens containing confidential student or employee information in view of others who do not have a legitimate educational interest in the data, or who do not have a bona fide business related need to have access to the data.

5. Not properly shredding any written or computer generated reports which contain student, employee or financial information.

6. Using the student, employee or financial information for personal business.

7. Allowing the use of a personal password by another individual who is not authorized to view the information.

8. Discussing the information contained in the student record outside of the University or while on the job with individuals who do not have a legitimate educational interest in the information (need-to-know); or discussing employee or financial information with others outside of the University or while on the job with individuals who do not have a bona fide business related need to have access to the information.

9. Leaving data displayed on an unattended computer screen while "logged on" to Banner.

Under no circumstances should an employee give confidential information about students or employees to any other students, to other employees, or to any other person who has not been authorized to receive such information by their position or by their departmental supervisor. Although directory information for students who have not requested privacy may be released without prior consent, any requests about students coming from other students or from anyone off campus should be referred to the Registrar.

Students and employees may request that directory or other personal information concerning them not be released. Under these circumstances, the “confidential” flag will be indicated on the student or employee record in Banner. Virtually no information may then be released without the student’s or employee’s express written consent. In some cases, releasing confidential information may threaten the safety of the student or employee.

I have read and clearly understand my responsibility to respect and maintain the confidentiality of all records and information to which I have been given access on the computer. I acknowledge the receipt of the security guidelines and further understand that the violation of these rules could result in disciplinary action, including suspension, termination and/or prosecution.

Name (Print) _____

Department _____

Signature _____

Date _____

Campus ID _____
(ex. W12345678)