Security Policy for Winthrop Employees with access to Student Information

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 student 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 student or employee data must understand and accept the responsibility of working with confidential student records.

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.

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.

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

Examples of inappropriate use of 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.

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. 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.

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.

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. 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_____