

All employees of the University of Nebraska at Kearney (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.

Access to the Student Information System (SIS) will be granted to those individuals who have been determined to have a legitimate educational interest in the data by the SIS Security Coordinator. Access to specific student data will be granted by approval of the SIS Security Coordinator and the Director of the Functional Area which oversees the student data being requested.

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

1. Every employee granted access to the system will use his/her assigned NU ID as username and his/her TrueYou password for authentication. 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, an employee must use his/her own authenticated session. When access to additional data or systems is needed, an employee shall make a request through the departmental supervisor to the SIS Security Coordinator. Each employee given access to student data is held responsible for any data which are input or retrieved under his/her username.
3. It is the responsibility of each employee to keep his/her password confidential and to change password whenever someone else may have obtained access to it.

A complete policy statement on the UNK implementation of FERPA guidelines can be found in the Registrar's Office. 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 the 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 the student's name, local and home addresses and telephone numbers, date and place of birth, major field of study, participation in officially-recognized activities and sports, dates of attendance, degrees and awards received, and the most recent previous educational institution attended.

Inappropriate use or misuse of student records is a violation of Nebraska Statutes and could result in civil and or criminal prosecution.

Examples of inappropriate use of student records are:

1. Accessing or reviewing a student's record without a legitimate educational interest.
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. Leaving reports or computer screens containing confidential student information in view of others who do not have a legitimate educational interest in the data.
4. Using the student information for personal business.
5. Giving your password to another individual not authorized to view the data.
6. 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).
7. Leaving data displayed on your computer while unattended.

Under no circumstances should an employee give confidential information about students 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 may be released without prior consent, any requests coming from students or from anyone off campus should be referred to the Registrar or the SIS Security Coordinator.\*\*

\*\* Students may request that directory information concerning them not be released. If that occurs, a FERPA flag appears. Virtually no information may then be released without the student's express written consent.

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.

**PRINT NAME** \_\_\_\_\_

**DEPARTMENT** \_\_\_\_\_

**SIGNATURE** \_\_\_\_\_

**DATE** \_\_\_\_\_