

COMPLIANCE STATEMENT FOR ACCESS TO STUDENT RECORDS

Responsibility of Registrar’s Office. The Office of the Registrar is the primary custodian of student permanent academic records and student data for the University. It is the responsibility of the Registrar’s Office to strive diligently to meet both its ethical and legal responsibilities to the University and its student body. To that end, the following regulations and guidelines governing access and protection of these records are effective for all offices and employees within the University of Connecticut. The principal governing legislation regarding these standards is the Family Educational Rights and Privacy Act (FERPA) of 1974, as amended.

The Family Educational Rights and Privacy Act of 1974, as amended, protects the privacy of educational records, establishes the students’ rights to inspect their educational records, provides guidelines for correcting inaccurate or misleading data through informal hearings, and permits students to file complaints with the Family Educational Rights and Privacy Act (FERPA) concerning alleged failures of the institution to comply with this Act. This statement clarifies the responsibilities of persons with access to student educational records.

Computer access. Your security passwords should remain confidential. You must log off or secure the system when leaving your computer workstation. Each individual will be responsible for the security of his/her PeopleSoft access code. It should NOT be given to any other person. If temporary help or student workers need to access PeopleSoft, access procedures must be worked out with the Systems Administrator. This statement must be filed with the Systems Administrator in the Office of the Registrar.

Confidentiality. You may access student records only as required to perform assigned duties. Within the University, anyone whose designated responsibilities require access may use information from student records for appropriate research, educational, or service functions. It is imperative that University personnel external to the Registrar’s Office understand the legal responsibilities they assume when they receive access to records or personal data in any form. To that end, each individual granted access to such data is required to sign this statement. The affidavit will clearly state their understanding of ethical and legal responsibilities.

To respond to an inquiry from outside the University, you must check whether the student has placed a current “directory suppress” on the record. Directory suppress is total suppression of information, including “public”. Unless explicitly suppressed by the student, the following “public” information may be released: student’s name, school or college, major field of study, degree sought, expected date of completion of degree requirements and graduation, degrees and awards received, dates of attendance, full or part time enrollment status, and the most previous educational agency or institution attended, participation in officially recognized activities and sports, weight and height of athletic team members, and other similar information.

All other information (including Social Security number) is private and may be released outside the University only with the student’s written permission. No information, public or private, on a student’s record may be released outside, except to an agent designated by the student. However, the Registrar’s Office, at its discretion, without a student’s written request, may release confidential information to the following: University officials having legitimate educational interest; Officials from other institutions in which the student seeks enrollment; Federal agencies; Public or private agencies regarding application for, or receipt of financial aid, including guaranteed student loans; Organizations conducting studies for educational agencies or institutions developing, validating, administering tests, student aid programs or educational improvement programs; Accrediting organizations; In compliance with a judicial order; Emergencies affecting the health or safety of the student or others.

Access to student information files. Staff granted access agree to:

- ◆ store information under secure conditions
- ◆ make every effort to ensure students’ privacy
- ◆ use information only as described in the request for data or access to student information system files;
- ◆ never represent summary data from files as “official” University data;
- ◆ department head or designated liaison must notify the System Administrator if an employee with access to the student information system is leaving the University, or is no longer serving in the intended capacity, so that his/her access can be deactivated.

Violations. If you violate this Compliance Statement for Access to Student Records, this constitutes grounds for rescinding your access to records or imposing disciplinary action, up to and including dismissal. Violations include the following offenses and any other comparable action:

- ◆ altering a student record without appropriate supporting documentation/authorization;
- ◆ accessing a student record outside of your assigned duties;
- ◆ releasing suppressed or private information without authorization;
- ◆ publicly discussing a student record in a way that might personally identify that student.

Employee acknowledgment. I have read the statement above and will comply with University policy on access to the student information system.

Employee name		Employee signature		Date	
Department		Campus mailing address (U-Box)		Phone Number	

Please complete the six blank boxes above, maintain a copy for your records, and return the original to: Janice Bazzani, Unit 5179, Storrs, CT. 06268-5179 or fax it to 860-486-2637.