

University of Connecticut

CONFIDENTIALITY/COMPLIANCE STATEMENT FOR ACCESS TO STUDENT DATA

The Family Educational Rights and Privacy Act (FERPA) of 1974, as amended, protects the privacy of student information contained in educational records, establishes students' rights to inspect their educational records, provides guidelines for correcting inaccurate or misleading data, and permits students to file complaints concerning alleged failures of the institution to comply with the requirements of FERPA. In addition, the University maintains a FERPA policy that provides further direction and explanation as how the provisions of FERPA apply at the University of Connecticut. All University faculty, staff, vendors, and volunteers who have access to and/or use student data must comply with the requirements of FERPA and the University's FERPA policy. This statement is meant to serve as a reminder of the responsibilities that those with electronic access to student records maintained in the Student Administration/PeopleSoft system(s) have under FERPA.

Computer access. Employee's security passwords should remain confidential. Each individual is responsible for the security of his/her Student Administration/PeopleSoft access code. It should NOT be given to any other person. If temporary employees or student workers need to have access to Student Administration/PeopleSoft, proper procedures must be followed according to University password policy (Your password is case sensitive: must include BOTH upper and lower, Minimum of 8 characters, can be up to 32 in length, contain at least one number (0-9), and one of the following special characters ! @ # \$ % ^ & * Note: the system remembers your last FIVE passwords and cannot match UserID or Email Address) and must be worked out with their systems administrator. Computer must be logged off or secured when leaving the workstation. Employees granted access agree to:

- store information with secure passwords
- make every effort to ensure students' privacy
- use information only as described in the request for data;
- never represent summary data from files as "official" University data-only OIRE provides official statistics;
- 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 no longer requires access as part of his/her job duties, so that his/her access can be deactivated.

The Office of the Registrar is the primary custodian of student permanent academic records and student data for the University. Any requests for copies of student records and/or academic information from students' Student Administration/PeopleSoft accounts should be directed to the Registrar's Office to determine appropriate responses.

Confidentiality. You may access student records only as required to perform assigned duties. Within the University, anyone whose designated responsibilities require such access may use information from student records for appropriate research, educational, or service functions. It is imperative that University personnel understand the legal responsibilities they assume when they receive access to records or personal data in any form.

Violations and/or any breach of confidentiality (including any discussions regarding student information on social networking sites, e.g. Facebook, MySpace, Twitter, Blogs, or any other internet related forum) **will** constitute grounds for rescinding your access to records and/or imposing disciplinary action, up to and including dismissal. Violations include the following and any other comparable action:

- The use of credentials for any reason other than official University business;
- Employee providing access and/or a password to another individual;
- Altering a student record without appropriate supporting documentation/authorization;
- Accessing a student record outside of your assigned duties;
- Releasing or otherwise sharing information in any manner prohibited by FERPA and/or other University policies without authorization;
- Discussing student information publicly in a way that might personally identify that student.

Employee acknowledgment. I have read and understand the statement above and will comply with University's policies regarding FERPA and access to student data on University information systems.

Employee name		Employee signature		Date	
Department		Campus mailing address (U-Box)		Phone Number	
NetID		Supervisor Name		PS Alpha Login ID	
<i>Office Use Only</i>		<i>SA User Type Category</i>		<i>PS ID</i>	

Please complete the blank boxes above, maintain a copy for your records, and return the original to:
Office of the Registrar, SA System Security Team, Unit 4077, Storrs, CT. 06268-5179 or fax it to 860-486-0272.