

FERPA: What faculty and staff need to know

It's the Law

FERPA (Family Educational Rights and Privacy Act) was passed by Congress in 1974, and it grants four specific rights to a post-secondary students:

- to see the information that the institution is keeping on the students;
- to seek amendment to those records and, in certain cases, append a statement to the record;
- to consent to disclosure of their records;
- to file a complaint with the FERPA Office in Washington.

Student Privacy Policy Office
U.S. Department of Education
400 Maryland Avenue SW
Washington, DC 20202-4605
PPRA.complaints@ed.gov

FERPA applies to the University of Minnesota because we receive federal financial aid funds.

Student Information Types

FERPA protects all Student educational records.

This includes information provided by a student for use in the educational process, such as:

- personal information (name, etc.)
- enrollment records
- student's exams or papers
- grades
- schedules
- class photos
- financial aid information

Directory/Public Information

Educational institutions may designate certain information as "directory" information. (See FERPA Regulations, Code of Federal Regulations, Title 34, Part 99.3).

Directory/Public Information is considered public and can be released without the student's written permission.

However, the student may opt to keep this information confidential.

Storage media for an educational record can include any of the following:

- document in the registrar's office
- electronic document or e-mail
- computer printout in your office
- class list
- computer display screen
- notes taken during an advising session
- database

It's Your Responsibility

As a faculty or staff member, you have a legal responsibility under FERPA to protect the confidentiality of student educational records in your possession.

- You have access to student information only for legitimate use in the completion of your responsibilities as a University employee. Need-to-know is the basic principle.
- With the exception of non-suppressed directory information, student educational records are considered private and may not be released without the written consent of the student.

- Student information stored in electronic format must be secure and available only to those entitled to access that information.
- Your access to student information is based on your role as a University faculty or staff member. You may not release lists or files with student information to any third party outside your college or departmental unit.

Directory information at the University Of Minnesota:

- Limited directory information
- Dates of enrollment
- Enrollment status
- College
- Class (i.e., freshman)
- Academic awards and honors
- Degrees received

Information not included in the list above is private student information and may not be released outside the University without the student's written permission or as otherwise provided in the Regents Policy on Student Education Records.

Can student directory or public information always be released? NO! Before releasing any information about a student, check PeopleSoft or APLUS for a student's suppression status. If the student has requested that directory information be withheld (suppressed his/her information), no information can be released. Note that FERPA does **NOT** require that directory information be released. University faculty and staff who have a need-to-know may obtain directory information for a student who has suppressed their information, but must not release this information.

How can a student withhold release of directory information? Students may request suppression of their information in MyU. First, log in to MyU, and select the "My Info" tab. Click on the pencil icon beside the "Directory Suppression" heading, carefully read the information that follows, then click the "Edit FERPA/Directory Restrictions" button. Select the desired suppression option, then click the "Save" button. The changes should be reflected on the "My Info" tab within the "Directory Suppression" section.

What are parental rights under FERPA? FERPA allows parental access to a student's educational records at the university level if the student grants written permission. Students may grant permission to share grades, billing, or other information in the My Info tab of MyU. Releasing other records such as advising records require written permission outside of MyU.

Where should I store my student data? Although you may be the one grading a student's performance, student data (e.g., grades, attendance, test scores) is owned by the University. It should not be stored on personal computing equipment, on the hard drives of shared computers, on portable devices such as "flash" drives, or on laptop computers. Portable devices are easily lost or stolen; if they contain student data when they are lost or stolen, all students may need to be notified. You should talk with your collegiate or departmental information technology support staff regarding secure data storage options.

How can student data be protected? Store all student data on a central, U of M server (not a Web server); password protect files; encrypt data on your computer; use anti-virus software; don't open suspicious attachments or links in e-mails; distribute graded materials in a secure manner; verify attachments and recipients before sending information via e-mail.

How are HIPAA and FERPA related? Medical documentation in the student education record is private information and is covered by FERPA. HIPAA (Health Insurance Portability and Accountability Act) regulations do not apply.

For more information Contact: ferpa@umn.edu

DO NOT!

- Use the Social Security Number or any portion of it, or the student ID number, in a public posting of grades or any other information;
- Leave graded tests, papers, or other student materials for students to pick up in a stack that requires sorting through the papers of all students;
- Discuss the progress of any student with anyone other than the student (including parents) without the signed, dated, and written consent of the student;
- Provide anyone with lists or files of students enrolled in your classes;
- Provide anyone with student schedules or assist anyone in finding a student on campus;
- Access the records of any student for personal reasons;
- Access the records of any student for any reason other than to perform your job duties.