

FERPA BASICS for Faculty and Staff



FERPA is the LAW. The Family Educational Rights and Privacy Act of 1974 (FERPA), as amended, is a federal law that safeguards the privacy of students' educational records. For a complete discussion of FERPA, please see the [FMU FERPA Policy](#).

All Francis Marion University faculty and staff are required under FERPA to protect our students' right to privacy and the confidentiality of their educational records.

Student records, other than those identified as Directory Information (see below), are subject to FERPA protection and therefore confidential. **Student records may not be released to or discussed with any third party without the written consent of the student.** FERPA-protected records include, but are not limited to:

- Social Security Number
- Race/ethnicity
- Gender
- GPA
- Grades or Performance in Class
- Papers, Quizzes, Tests, or Other Assignments
- Class Schedules
- Disciplinary Records
- Financial Information
- Country of Citizenship/nationality
- Religion
- Academic Standing

FERPA and Directory Information

FERPA permits the release of "directory information" without the student's prior written consent. Please note that students have the right to opt-out of disclosure of directory information. Contact the Registrar's Office if you have questions. FMU has designated the following items as "directory information:"

- Student name
- Enrollment status
- Major field of study
- Dates of attendance
- Degrees and awards received
- Eligibility for honors societies
- Most recent previous institution attended
- Mailing address
- Telephone listing
- FMU email address
- Date and place of birth
- Photograph
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams

If you are in doubt about a request for student information, contact the Registrar's Office for guidance.

How to Stay FERPA-Compliant

To meet FERPA requirements and protect the confidentiality of your students' records, you should NEVER do the following:

- Use students' social security numbers or student IDs to publicly post (on an office door, for example) grades or any other personal information about students
- Link a student's name with their university ID number in any public setting
- Discuss a student's progress with anyone (including parents) without the student's written consent
- Return graded papers in a manner in which a student has an opportunity to see another student's grade
- Call out grades or scores in class
- Provide the names or contact information of the students in your classes to a third party vendor
- Provide a student's schedule or whereabouts to anyone other than university employees to locate a student on campus. (All third party requests to find a student on campus should be directed to Campus Police)
- Access a student's record for personal reasons
- Store confidential student records on a computer unless your access to the computer is secure (for example, password-protected)
- Leave hard copy student records, like assignments or transcripts, in public view in your office