

FERPA GUIDANCE

for: Risk Assessments

Prepared for University of Florida Faculty & Staff

Document 1: Beyond the Gradebook – Identifying FERPA-Protected Data

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. A common misconception is that FERPA only applies to a student's final grades. In reality, an educational record is defined broadly as any record that is directly related to a student and maintained by the university, or by a third party properly acting on the university's behalf.

When evaluating technology for classroom, research, or administrative use, you must consider all forms of student data the application will collect, store, or process. FERPA-protected data extends far beyond grades and includes:

Data Category	Examples of Protected Information
Academic Work & Evaluations	Submitted assignments, exams, advising notes, and academic integrity records.
Logistical & Scheduling Data	Class rosters, personal class schedules, and attendance records.
Identifiers	Social Security Numbers (SSNs), UFIDs, and biometric records.
Financial & Admin Records	Financial aid information, billing history, and disciplinary records.

Key Takeaway

If a third-party application ingests, stores, or processes any of this information, it triggers strict FERPA compliance requirements that must be addressed during the Integrated Risk Management (IRM) review process.

Document 2: Directory vs. Non-Directory Information at UF

Not all student data requires the same level of restriction. FERPA categorizes information into two distinct classifications: Directory Information and Non-Directory Information.

Directory Information

This is data that is generally not considered harmful or an invasion of privacy if disclosed. The university may release directory information to the public without the student's written consent only for the categories it has formally designated as directory information in its annual FERPA notice to students, and only when the student has not requested a "Privacy Hold" through the Office of the University Registrar. At the University of Florida, directory information is strictly limited to:

- Student name, class, and college
- Local, permanent, and email addresses
- Listed telephone number
- Enrollment status and dates of attendance at UF
- Most recent previous educational institution attended
- Majors, minors, certificates, and specializations
- Degrees, honors, and awards earned
- Nature and place of employment at the university
- Publication titles
- Participation in officially recognized activities and sports
- Weight and height of university athletes

Non-Directory Information

Non-directory information comprises all other educational records (including the examples outlined in Document 1, such as UFIDs, schedules, and grades). This data is strictly confidential. It cannot be shared with third parties without explicit student consent or a legally valid contractual exception.

Even properly designated directory information loses its releasable status and requires written consent if a student's SSN or other non-directory information is used, alone or combined with other data elements, to identify the student or the student's records.

Document 3: Risk Assessments and Third-Party Compliance

Many IRM requests are delayed because the risk assessment fails to account for FERPA data protections. When you submit a request for a new third-party software, cloud service, or application that will process Non-Directory Information, the university must ensure that data remains legally protected.

To successfully pass a risk assessment involving FERPA-protected data, your request must include one of two compliance mechanisms:

Contractual Language (The FERPA Addendum)

The most common and efficient way to use third-party tools is under FERPA's "School Official" exception. For a vendor to qualify as a school official, the university must execute a formal FERPA Addendum alongside the main contract. This contractual language legally binds the vendor to ensure they:

- Perform an institutional service or function for which UF would otherwise use employees.
- Operate under the direct control of the university regarding the use and maintenance of education records.
- Are strictly prohibited from using the data for unauthorized purposes (such as marketing, profiling, or selling data) and from re-disclosing the personally identifiable information to other parties.
- Are granted access only to education records in which they have a legitimate educational interest. UF defines who qualifies as a school official and what constitutes a legitimate educational interest in its annual FERPA notification and must use reasonable methods to limit each vendor's access to only those records it needs.

Student Consent

If a vendor refuses to sign a FERPA addendum or accept UF's contractual data protection standards, the technology cannot be used under the School Official exception. In this scenario, you must obtain explicit, written consent (signed and dated) from every student prior to using the tool.

If choosing this route, your risk assessment must include a copy of the consent waiver the students will sign. The waiver must explicitly state:

- What specific data is being shared.
- The purpose of the disclosure.
- The identity of the specific third-party vendor receiving the data.

Note

Proceeding without a signed FERPA addendum from the vendor or a standardized consent waiver for students means the technology does not meet UF's privacy requirements for handling non-directory educational records.