Family Educational Rights and Privacy Act (FERPA) for Teaching

FERPA is a federal law that protects the privacy of enrolled and former student education records.

Key points when considering FERPA in the classroom:

- At the post-secondary level, all students have a right to confidentiality when it comes to their education record.
- Only those university officials with a legitimate educational need should have access to student education records.
- Although students can elect to have their directory information kept confidential, doing so will not/should not allow them to be anonymous within a class. Their directory information may be disclosed within the class as necessary.
- Make sure any third-party tools you use to conduct class have been approved for use by the university.

Education Records: May be maintained in multiple mediums, and include any record, with certain exceptions, maintained by an institution (or a contracted third-party) that is directly related to student(s) and can contain name or any information from which an individual student can be personally identified.

- Review the Texas A&M University approved list of third-party vendors at https://lms.tamu.edu/Menu/Teaching-Tools/Third-Party-Tool-Status

Directory Information: Education record information that is generally considered not harmful to students if publicly released. Review the Texas A&M University published list of items falling under Directory Information at https://registrar.tamu.edu/about-us/policies/ferpa

- Students may place directory holds on their directory information.
- Students with directory information holds are noted by “Confidential” listed by their name on Howdy course rosters.

Non-Directory Information: Education record information deemed more sensitive than directory information, including course schedule, course roster, grades, test scores, etc.

WHAT DOES THIS MEAN FOR TEACHING ACTIVITIES?

Posting Grades:

- Public posting of grades either by the student’s name, UIN, SSN, or any portion of these numbers without the student’s prior written consent is a violation of FERPA. This includes publicly posting grades to a class/institutional website.
- Even with names obscured, numeric student identifiers are considered personally identifiable information. The practice of posting grades by SSN, UIN, or any portion of these numbers violates FERPA.
- Never post grades, even if coded, in alphabetical order or any other recognizable order.
- There is ***no guarantee of confidentiality*** when sending grades via email or the Internet. FERPA is a privacy law, not an IT security law. As such, FERPA does not explicitly prohibit use of email to transmit protected student information. However, the institution would be held responsible if an unauthorized third party gained access, in any manner, to a student's education record through any electronic transmission method, so information sent via email should be secured and not allow disclosures to third parties not authorized by the student, including parents or guardians, significant others, roommates, or other individuals who may have access to email for the purpose of IT support (e.g., Yahoo! employees).
- Per IT Security policy, university data classified as confidential or higher that is transmitted in an email message must be encrypted. Education record data is one such data type included within the confidential data classification. In order to ensure compliance with FERPA, we recommend to utilize Filex for document transfer of sensitive data or to encrypt emails with confidential information.
- To avoid the risk of unauthorized access, only secure web sites which require authentication (howdy.tamu.edu) should be used for accessing grade information.

In-Class Activities:

- Do not circulate a printed class list with student name and social security number/institutional identification number as an attendance roster.
- Do not leave graded tests or papers in a stack for students to pick up by sorting through the tests or papers of all students.
- Providing student examples of work in class is allowable if you 1) remove all identifiers so the work cannot be reasonably tied to any student, OR 2) obtain written consent from the student to share their work.

Family Educational Rights and Privacy Act (FERPA) for Teaching

Contact from a student by phone:

- Try to avoid discussing confidential information by phone as much as possible. Doing so in itself is not a violation of FERPA but should the information you provide by phone be disclosed to someone other than the student, that could result in a FERPA violation.
- During phone conversations, avoid looking up the student's record. Instead, try to provide more general help.
- Utilize "if" statements (e.g., "IF you did not submit the assignment by the deadline, the grading penalty is ….") to provide more specific information by phone.
- Verify the identity of the student (ask questions only the student could answer, such as the name of the course, an example of an assignment from the course, recent discussions in class or questions from an assignment).
    - If there is uncertainty about the student's identity, err on the side of caution and have them email you a request for the information. The email must be received from the student's @tamu.edu account.
        - An email request ensures the student has documentation of the information being requested, and answers provided.
        - Dual authentication with university email allows for identity verification.

Contact from a student by email:

- Verify the identity of the student (utilizing their university provided email (@tamu.edu) account).
    - Dual authentication allows for identity verification.
    - An email ensures the student has documentation of the information being requested, and answers provided.
    - TAMU Student Rule 61 establishes email as an official means of communication for Texas A&M University.
- Follow IT Security policy, which indicates university data classified as confidential or higher that is transmitted in an email message must be encrypted. Education record data is one such data type included within the confidential data classification. To ensure compliance with FERPA, we recommend utilizing Filex for document transfer of sensitive data.

Some guidance to prevent a potential FERPA incident

- Have the student contact you via their university email (@tamu.edu) account or utilize Canvas messaging.
- Never discuss the progress of any student with anyone other than the student (including parents/guardians) without the consent of the student.
- Never provide anyone with student schedules or assist anyone in finding a student on campus.
- Never provide anyone with lists of students enrolled in your classes for any commercial purpose.
- Do not email class rosters.
- Do not provide directory information about a student who has requested a directory hold.
- Do not include FERPA protected information in a letter of recommendation/reference without the student's written permission (this includes enrollment in a particular course, student GPA, or grade in a specific course).

FERPA REPORTING FACTS

FERPA incidents, at any level, need to be submitted to the Office of the Registrar FERPA Incident Team for review (ferpa@tamu.edu).

FERPA incidents can include accidental and unintentional disclosure of student education records (examples include student data left laying out on a desk in plain view, unauthorized access to information on computer monitors, student education records left on shared printers).

The FERPA Incident Team will collect information related to the incident, determine if the incident is a FERPA violation, and provide a plan of action for notification and remediation of the issue.

Always ask the FERPA Incident Team questions if you are unsure of how to handle a situation or if an incident needs to be reported. This team is in place for assistance of this kind.

What needs to be reported and when should you reach out to the FERPA Incident Team?

- FERPA Incident or Violation
- FERPA Inquiries (asking for guidance on a situation)