

Family Educational Rights and Privacy Act (FERPA) for Academic Advising

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

Key points and language to use when discussing FERPA:

- Students own their own data (education record) in higher education spaces (even if under 18 once enrolled in higher education). *Education records* may be maintained in multiple mediums, and include any record, with certain exceptions, maintained by an institution that is directly related to student(s) and can contain name or any information from which an individual student can be personally identified.
- We serve as stewards of their data
- Confidentiality rules have shifted for students and parents/guardians
 - Parents own the data (education record) in K-12
 - Now the student owns their data (education record)
 - This change can be difficult for some parents/guardians - utilize empathetic responses
- Certification of Dependency Form
 - Compass form
 - **SOAFOLK** (look for the X code with the description of “Registrar Certified Dependency”)
 - Other codes are used for other items and come from applications and other avenues
 - Q code is used primarily by Qatar to show FERPA Designees based on agreements with individuals in Qatar
 - Howdy Dashboard for student
 - Select ‘Overview’ and any individuals verified by the submission of a Certification of Dependency Form are listed under the ‘Biographic Information’

CHECKLISTS FOR ACADEMIC ADVISORS, FACULTY, AND STAFF

General Recommendations:

- 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 referencing or looking up the student’s record. Instead, try to provide more general help.
- Utilize “if” statements (e.g., “IF you failed the prerequisite, you will not be able to register for the course.”) to provide more specific information by phone.

Contact from a student by phone:

- Verify the identity of the student (ask for DOB and major, continue asking non-directory information questions until comfortable with identity of caller - **NEVER ask SSN**).
 - 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
 - This way the student has documentation of the information being requested, and answers provided.
 - Dual authentication with university email allows for identity verification
- Make sure to understand the exact question (ask questions) to provide the best/most accurate information.
- Request the student to make an in-person or virtual appointment with you to discuss further details and information.
- When in doubt, don’t give it out! Review “General Recommendations” section.

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.
 - This way 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.

Family Educational Rights and Privacy Act (FERPA) for Academic Advising

Contact from a third party (parent, sibling, spouse, etc.):

- Ask if the student is there so you can speak to both/all of them. It is recommended to speak with the student personally.
 - Siblings, spouses, and other third parties will not be authorized for a release of education record information under the Certification of Dependency, as they are not parents/guardians and do not qualify for the verification under the Certification of Dependency Form.
 - If student would like to release information to these parties, a signed education record release should be provided by the student (outlining what information can be released, to whom, for what purpose, and for how long)
- For university officials, determine if there is an educational need for the release of information
 - When in doubt, contact the Office of the Registrar FERPA Team: ferpa@tamu.edu
- Check SOAFOLK for Certification of Dependency
 - Verify the identity of the caller as someone authorized to receive student education records (ask for DOB and major, continue asking non-directory information questions until comfortable with identity of caller while not disclosing student information- **NEVER ask SSN**).
 - Even with consent, what information should you provide?
 - Are you comfortable giving out the information?
 - How would you want the situation to be handled if it was your information?
 - Consider the circumstances of the request.
 - How serious is the situation?
 - Is it time sensitive?
 - Is it something the student should be handling personally?

Some guidance to prevent a potential FERPA incident

- Have the student contact you via their university email (@tamu.edu) account.
- Make every attempt to keep the answers to third parties as general as possible, but still answer the questions.
- If uncomfortable, explain you are not comfortable giving that information out.
- Remember that FERPA permits disclosing to authorized individuals, but it does not mandate it.
- When in doubt, don't give it out!
- Refer third party to your supervisor or the Office of the Registrar FERPA Team: ferpa@tamu.edu

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