FERPA Basics: What Faculty and Staff Need to Know About FERPA

The Family Educational and Privacy Rights Act of 1974 ("FERPA") is the federal law that protects a student's privacy with respect to his or her education records. An education record is any recorded information that personally identifies and is related to a student, and is maintained by the University. Because of FERPA, faculty and staff must take care in how they handle students' education records (including any information in education records).

The University of Dayton has adopted a policy regarding its implementation of FERPA, referred to as its Policy on Disclosure of Education Records. Among other things, the policy provides key definitions, outlines students' rights and identifies which University offices are responsible for various categories of records. Further, the University annually notifies students of their FERPA rights by publishing those rights in the Student Handbook.

How FERPA plays out in day-to-day academic life might not be obvious from the law itself, the University's policy and the annual students' notification of rights. This "FERPA Basics" document is meant to help you navigate how FERPA comes into play with respect to some typical University activities, duties and discussions. By no means, however, does this document address all issues you may confront nor does it address all FERPA "exceptions." Thus, if you have questions regarding FERPA after reviewing this document as well as the University's FERPA policy, you may wish to consult the Registrar's Office or the Office of Legal Affairs.

Here are some basic points to keep in mind:

- **FERPA covers more than just transcripts and grades.** FERPA covers any record that personally identifies a student and is retained by the University. This means that class schedules, disciplinary records, financial account information (including financial aid records), photographs and even emails are considered educational records. When in doubt, assume that information (in whatever form) about an individual student is an educational record.
- **Student records can be disclosed to other University officials who need the information to perform their duties for the University.** This means that faculty members can turn grades over to the Registrar's Office; employees who observe disciplinary violations can report those to Student Development; observed mental health concerns can be reported to Student Development/Counseling Center (and to the Threat Assessment Team and/or Public Safety, if necessary); etc.
- **If a health or safety emergency exists, otherwise FERPA-protected information may be disclosed to those with a need-to-know to address the emergency.** FERPA permits the disclosure of protected information when the University has a good-faith belief that a health or safety emergency exists.

- **A student's academic performance should never be the topic of water-cooler talk.** Keep in mind the general rule that records can be disclosed for "legitimate educational interests." If you are catching up with a colleague in a completely different department whose neighbor's son is in your class, there is no reason to share how the neighbor's son is performing in your class. Conversations about students that do not forward a legitimate educational interest generally run afoul of FERPA.
- **Just because information does not contain a student's name does not mean it falls outside of FERPA.** For example, if a record contains a student's gender, major, class year and residence, it likely contains enough information to personally identify that student and thus fall under the reach of FERPA. Or if information is listed about a group of students without their names but in such a way that a clever observer could identify who's who (i.e., the list is in alphabetical order but with the names omitted), then such a list – if made public – would disclose educational records in violation of FERPA.
- **Even if you think the information is generally releasable "directory information," check before disclosing.** "Directory information" includes information such as a student's name, phone numbers, major, etc.; see the University's Policy on Disclosure of Education Records for the full definition. Directory information generally can be disclosed, except a student can opt that his or her own information not be disclosed. Thus, before disclosing directory information about a student, you should check with the Registrar's Office to see if the student has opted to keep that information from being disclosed. Also, note that directory information should not be disclosed in such a way as to release protected information; e.g., if someone asks for the directory information of students with a GPA of 3.0 or higher, you cannot provide the requested information as that would reveal protected information (that is, students with 3.0 or higher GPAs).
- **Err on the side of obtaining a FERPA release form (or confirming that one is on file by checking the notes section of DegreeWorks).** If you receive a request for a student's education records from someone other than the student, and the requester is not a University official with a legitimate educational interest in the record, then take steps to have the student consent to the release of records in writing (or check whether a form permitting such release is already on file). A FERPA consent to release form is available here. Once filled out and signed by the student, the form contents should be uploaded to DegreeWorks by a FERPA "custodian" or "gatekeeper," and then it should be submitted to the Registrar's Office.

- **Err on the side of putting control of a record in the student's hands. If** a parent contacts you directly about a student's performance, and you do not know if the student has signed a waiver, try saying to the parent, "Why don't you ask your [son/daughter] to talk to me about the issue?" or "I recommend that you ask your [son/daughter] to sign this FERPA release, and then we can talk."

With these points in mind, here's a practical list of what to do and not do when it comes to student records:

DO	**DO N'T**
• Do use the University's Learning Management System, Isidore system or self-service Banner (via Porches) to post grades	• Don't use systems other than the University's Learning Management System, Isidore or self-service Banner to post students' grades
• Do use a sealed envelope if you need to send out student information	• Don't post grades by SSN or student ID number either physically (e.g., printed sheet on office door) or electronically (*e.g.*, website that you maintain)
• Do obtain a signed release form from a student before releasing records to someone who's requested that student's records	• Don't send out student information on a postcard
• If you have a good-faith belief that a health or safety emergency exists, then do release records necessary to deal with that emergency situation	• Don't discuss a student's information in such a way that others might overhear
• Do use a student's udayton.edu email address for correspondence you need to send to that student	• Don't send grade information or other student details to a student at an email address you don't recognize to be theirs (the safest way is to use a student's udayton.edu address)
• Do use *your* udayton.edu email address for correspondence you need to send out in your role for the University (other systems may not be as secure as ours)	• Don't release information about a student by phone or email without first confirming the identity of the recipient
• Do protect your log-in password	• Don't leave student information where it could be seen or accessed by others
	• Don't leave student papers or tests in a pile for students to sort through to pick theirs up

DO (continued)

- If someone calls you requesting educational record information, do go through steps to verify that the person on the phone is who the person claims to be (*i.e.*, the student him/herself, or someone the student has authorized to have access to such information)
- Do keep your computer locked when you're not in your office
- Do set your handheld devices (including smartphones and tablets) to automatically lock when not in use for a period of time

DO N'T (continued)

- Don't dispose of student records in ordinary trash
- Don't access Banner to find out information about a student for reasons unrelated to your University duties
- Don't share your UD password (not even with student employees)
- If your child is a student at UD, don't use your University resources/access to look up your child's records unless you have your child's consent
- Don't leave your computer or handheld device unlocked when you're away from them

This list is meant to assist you in dealing with the most common issues that arise under FERPA. If you have questions that this guidance does not answer, please feel free to contact the Registrar's Office (9-4141) or the Office of Legal Affairs (9-4333) for further assistance.