FERPA - Protect Yourself - Understanding the Privacy of Student Records
About this Course
FERPA - Protect Yourself ... and Your Students

This course is designed to give you an overview of the federal law on student records and UAB related policies, as well as the guidelines for the appropriate use of student records.
Course Instructions

It is suggested that you:
1. Begin by reading the 'FERPA - A Faculty and Staff Tutorial' material.
2. Complete the FERPA 'Test Your Knowledge' quiz.
3. Read through and refer to the material in the Resource Center for your reference.

If you are having technical problems, contact the
• AskIT Help Desk at 996-5555 (6-5555 on campus)
• e-mail askit@uab.edu

If you have specific questions regarding FERPA or any other policy listed in this course, please contact
• Tina Collins
  University Registrar
  934-8152
  collinst@uab.edu or
• Cary Wahlheim
  UAB Legal Counsel
  934-3474
  ctw@uab.edu

Please note that clicking any links in the courses will open a new browser window. You may close this window by clicking the 'x' in the upper right corner. However, be careful not to close your course window until you are ready to exit the course.
UAB FERPA Website
UAB FERPA Website

Click [here](https://www.uab.edu/studentaffairs/ferpa) to visit the UAB FERPA Website.
FERPA - A Faculty and Staff Tutorial
What is FERPA?

The **Family Educational Rights and Privacy Act of 1974**, commonly known as **FERPA**, is a federal law governing the privacy of educational records.

It grants specific rights to students and puts restrictions on how schools may handle educational records.

FERPA rights apply to students, regardless of age, who are in attendance at a postsecondary institution, and to former students.
Why is it important for you to know about FERPA?

Many faculty and staff have access to restricted student information, and the consequences of how we handle, or mishandle student information are significant. Any educational institution that receives funds under any program administered by the U.S. Secretary of Education is bound by FERPA requirements. Funds administered by the Secretary of Education may be withheld from an institution that fails to comply with FERPA requirements.

**The Essence of the Act:**

- College students must be permitted to inspect their own educational records.
- School officials may not disclose personally identifiable information about students nor permit inspection of their records without written consent unless such action is covered by an exception permitted by the Act.
FERPA – Key Concepts and Terms

Key Concepts:
• Written consent required for disclosure of student record information
• The exceptions to written consent of student
• Students’ rights to access their records
• Parents/parental disclosure
• Legitimate educational interest

Key Terms:
• Educational Record
• Personally Identifiable
• Directory information
• School Official
**What are a student’s rights under FERPA?**

**FERPA gives students the right to:**
- Inspect and review their educational records within 45 days of a request
- Seek the amendment of educational records if they are inaccurate or misleading, and in certain cases the right to append a statement to their records
- Prevent the disclosure of their own educational records
- File a complaint with the FERPA Office in Washington, D.C.

The institution is required by the Act to provide annual notification to students of their FERPA rights.
What are educational records?

Educational records are records that are maintained by the University as part of the educational process.

Examples of educational records include personal information, enrollment records, grades, and schedules.

**Student educational records include:**
- A paper document in the Registrar’s Office
- A computer print-out in your office
- A class list on your desktop
- A computer display screen
- An e-mail message
- Notes you have taken during an advisement session if they have been viewed by someone other than yourself (unless that person is serving as your temporary substitute)
- A verbal exchange
What are NOT educational records?

**Student educational records do NOT include:**

- Private notes you have made on a student and intended for your sole possession, known as sole possession notes
- Campus police records
- Employment records when employment is not contingent on being a student
- Medical records
- Records maintained by counseling staff
- Post-attendance records (e.g., alumni records)

**Student information must be handled with the same care, regardless of whether it’s used in written, electronic, or verbal form.**

Note that employment records are considered educational records if the individual is employed as a result of his/her status as a student (e.g., work study).
What are sole possession notes?

Sole possession notes are made by one person as an individual observation or recollection, that are kept in the possession of the maker, and are shared only with a temporary substitute.

- This term has always been narrowly defined.
- Notes taken in conjunction with any other person are not sole possession notes (counselor’s notes, interview notes).
- Sharing the notes with another person, or placing them in an area where they can be viewed by others makes them “education records” and subject to FERPA.
- **Best advice:** If you don’t want it reviewed, don’t write it down.
Scenario 1

You are an academic advisor, and you regularly make notes about your meetings with students. You keep these notes in each individual student’s file. The notes may include observations you’ve made about an academic deficiency a student should address or a reference to a non-school related personal problem, like financial difficulty. A student has come to you expressing some concern that a work study in your office may have access to her personal information, and she wants to see what is in her file. You agree, but you remove your meeting notes because you consider them ‘sole possession notes’ under FERPA.

Are you abiding by FERPA regulations?

NO. If these notes were not shared with anyone other than a temporary substitute and remained in your sole possession, they would not be considered educational records and would not have to be disclosed. However, if the notes are part of a student’s regular file and if they are put in a location where they can be accessed by others, they become educational records and are subject to FERPA regulations.
What is personally identifiable information?

**Personally identifiable** means data or information which includes, but may not be limited to:
- The name of the student, the student’s parent, or other family members
- A personal identifier (such as a social security number or student number)
- A list of personal characteristics or other information which would make the student’s identity easily traceable

One of the main emphases of FERPA is that personally identifiable information in an educational record may not be released without prior written consent from the student. The Act does provide several exceptions to this consent requirement.

One of the primary exceptions is that an institution may disclose personally identifiable information without written consent to school officials whom the institution has determined to have a legitimate educational interest.
Who is considered to be a school official?

A school official is a person:

- Employed by the University in an administrative, supervisory, academic or research, or support staff position
- A person or company with whom the University has contracted (such as an attorney, auditor, or collection agent)
- A person serving on the Board of Trustees
- A student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.
Directory Information

FERPA defines as “Directory Information” the information that may be released without specific written permission from the student, except in certain cases specified by the regulations. The UAB Student Records Policy defines the following items as Directory Information:

- Name
- Address (local and permanent)
- Telephone number
- University e-mail
- Date and place of birth
- Major field of study
- Participation in officially recognized activities and sports
- Dates of attendance
- Degrees and awards received
- Institution most recently previously attended
What kind of student information may be disclosed?

FERPA defines Directory Information as the information that may be released without specific written permission from the student, except in certain cases specified by the regulations.

The UAB Student Records Policy defines the following items as Directory Information:

- Name
- Address (local and permanent)
- Telephone number
- University e-mail
- Date and place of birth
- Major field of study
- Participation in officially recognized activities and sports
- Dates of attendance
- Degrees and awards received
- Institution most recently previously attended
Withholding Directory Information

At the student’s written request, directory information may be withheld on a limited or complete basis.

A student may request non-disclosure of directory information, which prevents the University from releasing any directory information except to school officials with legitimate educational interests — a “need to know” — and certain others as specified in the regulations.

Non-disclosure:
A student may request full non-disclosure, which prevents the University from releasing any directory information except to school officials with legitimate educational interests — a “need to know” — and certain others as specified in the regulations.

A non-disclosure request will generate a pop-up Confidential warning in Banner when first accessing the record, and the word “Confidential” will remain above the student’s ID in the key block, as shown in the image.
What is non-directory information?

Non-directory information is any educational record not classified as directory information.

Examples of non-directory information include:
- Religious affiliation
- Citizenship
- Disciplinary status
- Ethnicity
- Gender
- Grade point average
- Marital status
- Social security number / student ID
- Grades / exam scores
- Test scores (e.g., SAT, ACT, GRE, etc.)

This private information must not be released to anyone (including parents of the student) without written consent from the student except under strictly defined conditions.

University faculty and staff may access this information only if they have a legitimate need to use it in fulfillment of official duties.

Requests from outside your department or school for non-directory information should be referred to the Office of the University Registrar.
**What is meant by legitimate educational interest?**

In accordance with FERPA, a school official has a legitimate educational interest if the official needs to review an educational record in order to fulfill his/her professional responsibility.

Legitimate educational interest does not convey inherent rights to any and all student information. Neither curiosity nor personal interest constitute a legitimate educational “need to know.”
Scenario 2

You are a faculty member. It is final grades time and your grades must be submitted in five hours. You have advising responsibilities in your department, so you have been given transcript access.

You use your logon ID for Banner to look at the transcripts of students in your class before assigning final grades because you want to get a “feel” for which grades were assigned to those students in the past.

Is this an appropriate use of Banner access?

NO. The determination of a student’s grade in a course should be based on performance in that course. The grades a student has earned in other courses should not be a factor in determining a final grade in your course. Using your ability to access to student information to view a student’s academic history is a misuse of that privilege. In this case, you do not have a “legitimate educational interest” in a student’s past academic performance.
What are some circumstances in which educational records may be released?

- In the event of a health or safety emergency, student information may be released to the appropriate authorities as required to protect the safety of students.
- Certain federal and state educational authorities may obtain educational records.
- Parents or guardians who can demonstrate by income tax returns that students are their dependents may be eligible to view records.
- The University may release student records in response to court orders or subpoenas.
- Military recruiters may request certain student information under the Solomon Amendment.
- **In all exceptional circumstances, the requestor should be referred to the Office of the University Registrar.**
Scenario 3

You work in the Registrar’s office. You receive a call from Dave and Kathy Smith, the parents of a former UAB student. Their son, Kevin, was dismissed over a year ago. Dave and Kathy live in Florida and have been paying for Kevin to attend your college for every term during the last three years, including room and board and out-of-state tuition. They called to see how things were going since they don’t hear much from Kevin about school.

How do you handle this conversation?

Prior consent is required to release anything but directory information. Since dates of attendance are considered directory information by UAB, this information may be disclosed unless the student has requested non-disclosure. An exception to the non-disclosure rule may be made if the parents can prove dependency by the submission of their most recent tax return. In this case they should be referred to the Office of the University Registrar.
Who is ultimately responsible for protecting a student’s privacy?

If you have access to student data, you are responsible for its proper handling.

No matter what the form or content, you are accountable for handling student records in accordance with the law and University policy.

You are responsible for making sure that the student data in your possession is secured.

Take measures to protect against unauthorized access to student data stored on a personal computer, a network, or any other storage media:

- Keep storage media in a secure, locked location.
- Restrict access to your computer.
- Never leave student data displayed on your computer screen.
- When you have finished a computer task involving student data, exit all files, sign off all applications, and close all application windows.
- Shared printed material that contains sensitive or restricted data.
Special considerations for storing student data on computers

Software used to create spreadsheets and databases is widely available to staff. In many cases, FERPA-protected educational records are entered into a computer manually by faculty and staff to serve a variety of departmental needs.

In addition, most computers are connected to a local area network. Under these circumstances, student data could be at risk from hackers who gain access to computers where it is stored.

Further, data could also be kept on departmental file servers, where the end user who compiled and stored the student data might not necessarily know who else has access to that network location.
‘Best practices’ for storing student data on computers

These situations require special precautions be taken when storing student data on a computer.

- Consult with your local computer support staff to insure that the location where student data is stored is secure, and that access to that location is controlled and monitored for unauthorized use.
- Ensure your computer support personnel keep your computer software and antivirus up to date.
- Ensure that your computer support personnel configures a firewall to protect your data.
- Use centralized file services rather than storing sensitive data on your local drive. Consult with your computer support personnel to ensure that shared areas are restricted to only authorized users.
- Some “free” software actually can present security risks, particularly free entertainment or utility software. Check with your computer support personnel before installing any such software.
- Network administrators should perform periodic scans of servers to look for newly-created files that contain sensitive student data, document the purpose of such files, and who can access them.
- Do not leave portable devices or media unattended.
- Do not store sensitive data on portable devices such as notebooks. Instead, have your support personnel instruct you on how to securely do remote access to your centralized file share.
- Do not email sensitive data in the course of business. Instead, mail the address of a secured centralized location to your recipients. The UAB Drop box is an example of a secure central location.
Scenario 4

Your Dean has asked you to compile a report that measures your school’s performance against UAB’s Strategic Plan goals for enrollment, composite ACT score and average GPA. You create an Excel spreadsheet and save it to a folder on your network so that secretaries can input name, student number, ACT score, and overall GPA for each student in their respective departments. When all data entry is complete, you email the spreadsheet to an assistant to be tabulated and formatted into a final report.

Is this an acceptable way of handling and storing this sensitive data?

No. You have no idea who has access to the file on that network location. It could be visible to many others, including students. You should work with your local IT staff to ensure that only authorized persons can access this network location. Second, you should never use email as a method of transferring a file containing sensitive information. There is no guarantee that the file you sent will be received by the person whom you intended. Instead, you should use software to electronically encrypt the file with a password, and then use the UAB Drop Box facility to deliver the encrypted file to the assistant. See https://dropbox.dpo.uab.edu for more information.
Are there special FERPA considerations for faculty?

There are some special “don’ts” for faculty to avoid violations of FERPA rules.

**DO NOT:**

- At any time use any portion of the social security number of a student in a public posting of grades.
- Publicly post or in any way make publicly available a list of grades for any work in classes with fewer than eight students.
- Link the name of a student with that student’s SSN in any public manner.
- Leave graded tests in a stack for students to pick up by sorting through the papers of all students.
- Circulate a printed class list with student name and BlazerID or grades as an attendance roster.
- Discuss the progress of any student with anyone other than the student (including parents) without the consent of the student unless that person’s official responsibilities identify his/her legitimate educational interest in that information for that student.
- Provide anyone with lists of students enrolled in your classes for any commercial purpose.
- Provide anyone with student schedules or assist anyone other than university employees in finding a student on campus.
- Include confidential information (i.e., grades, number of credits) in a letter of recommendation without the written consent of the student.

Click [here](#) to view about the UAB’s official policy on the public posting of grades.
Scenario 5

You are a departmental secretary and you receive a call a few days into the semester from an adjunct instructor who has misplaced his class roll. He needs a copy of this roll to create a grade book and wants to make sure that he has included all officially enrolled students. He asks you to fax a copy of the roll to his wife’s office, where her very efficient secretary will be on the look-out and make sure his wife receives it.

If you do as the instructor requests, are you violating FERPA rules?

YES. Class rolls carry personally identifiable information, including student numbers. Faxing a class roll to someone who does not have a legitimate educational interest in this information is a violation of FERPA.
Letters of Recommendation

Statements made by a person making a recommendation that are made from that person’s personal observation or knowledge do not require written release from the student who is the subject of the recommendation.

However, if personally identifiable information obtained from a student’s educational record is included in a letter of recommendation (grades, GPA, etc.), the writer is required to obtain a signed release from the student which:

• specifies the records that may be disclosed,
• states the purpose of the disclosure, and
• identifies the party or class of parties to whom the disclosure can be made

Since the letter of recommendation would be part of the student’s educational record, the student has the right to read it — unless she/he has waived that right of access.

Note that obtaining a written consent from a student to discuss his/her academic performance with third parties is recommended, even though not necessarily required.

Click here to view the letter of recommendation release form.
Disciplinary Matters

Disclosure of disciplinary information in a student’s educational record is allowed under certain circumstances.

Institutions may disclose educational records without written consent of the student to parents of a student under the age of 21 regarding a violation of any law or institutional policy or rule governing the use of alcohol or a controlled substance.

Institutions may publicly disclose educational records without written consent of the student regarding the final results of an institutional disciplinary proceeding as long as the student has been determined to be the alleged perpetrator of a violent crime or non-forcible sex offense.
A Brief Review

• You are responsible for protecting student data in your possession.
• Educational records may not be released without the written consent of the student.
• Individual directory information may be released without written consent, except when a student has filed a nondisclosure / privacy request. Suppressed information may not be released.
• University employees may access and use private educational records only as necessary to conduct official business that is related to the educational interest of the student.
• Take appropriate measures to protect student records that are stored on personal computers and local networks.
• **If in doubt, do not release information about a student. Refer requests to the Office of the University Registrar.**
Resource Center

- UAB Policies Related to Student Records
- UAB Student Records Policy
- UAB Grade Posting & Distribution Policy
- Request to Withold Directory Information (PDF)

(Click the links above to view and download important resources.)
Course Quiz
Course Quiz Instructions

The Test Your Knowledge quiz will take approximately 10 minutes to complete. A score of at least 75% (Total score: 100/130) is needed to ensure you receive course completion status. If you score less than 75%, please try the quiz again, as multiple attempts are allowed.

Please note that although the score on your quiz is private information that is not shared with anyone, your actual completion of the quiz will be noted by the Institutional FERPA Coordinator, as well as the Dean and Provost.

Please exit the course to take the post-assessment test. To exit the course you can either close the browser window or click on the "x" located in the right top corner.