A FERPA Audit

Do you wonder if your campus is meeting general expectations regarding FERPA? Use the following questions/checklist to do a basic self-assessment of your office and/or your campus.

Who on your campus is responsible for FERPA compliance?

Typically, this responsibility falls to the registrar's office, but Legal Affairs or Academic Affairs might also hold it.

If you are the "point person" for FERPA on your campus, have you received appropriate training?

* AACRAO sponsors FERPA workshops throughout the year at various locations across the country. Visit the AACRAO Web site (www.aacrao.org) for details.
* FERPA is always a topic for several sessions at national AACRAO meetings.
* Other professional organizations [*e.g.*, state/regional divisions of AACRAO, the Council on Law in Higher Education (CLHE)] sponsor FERPA-related sessions or presentations each year.
* Have you read this publication and understand the important concepts and terms within FERPA that are found here?

What resources can you utilize in addressing FERPA issues on your campus?

* Do you have a Legal Affairs or General Counsel resource (with someone on staff who is knowledgeable about FERPA)?
* Professional colleagues, professional associations, *e.g.*, AACRAO, the National Association of College and University Attorneys (NACUA), CLHE, and publications from those entities are excellent resources. For example, NACUA has published an outstanding complement to this publication: *The Family Educational Rights and Privacy Act: A Legal Compendium* by Stephen McDonald.
* The Family Policy Compliance Office in the U. S. Department of Education — particularly given its expanding Web site materials — is an excellent resource for information and answers to problem situations. The Web site is www.ed.gov/policy/gen/guid/fpco/index.html.
* The federal guidelines (known as the regulations) regarding FERPA are also helpful.

Do you have a records retention plan?

While FERPA does not include a records retention plan, it does have direct impact on access to and use of existing records. Having an up-to-date records retention plan is good policy for any office that regularly works with important institutional records. For example, under FERPA, if students request access to their education records, you can't destroy those records, if they still exist, until after the student has seen them. You can, however, tell a student who has requested to see his education records that those records have been destroyed (if that has occurred), as long as they were destroyed in accordance with the institution's records retention plan. AACRAO's *Records Retention Guide* is an excellent resource if you do not already have it in your professional library.

What security policies and protocols do you have in place on your campus?

* This is a critical area related to FERPA, particularly in this age of greater reliance on technology.
* Who is responsible for security controls and policy decisions regarding security in your networked/electronic environment?
* Ideally, you should establish security controls which limit access to those who should/need to have access in order to do their jobs. This refers to the FERPA concept of "legitimate educational interest" or the "educational need to know." In many older systems, student database maintenance is more tightly controlled than providing users viewing access to student records; therefore,

consider both viewing and maintenance capabilities.
* Perform an analysis of roles and security-related decision-making procedures on your campus. For example, you are likely to have "sets" of common security protocols for staff advisers, faculty, office processing staff, student staff, etc. Once established, such "sets" make it easier to administer and manage security issues.

What training requirements and policies do you have in place regarding FERPA and student records?
* Do you have mandatory training for persons who will have access to student records — particularly via technology?
* If so, must/should that training occur prior to receiving access (*e.g.*, the staff person doesn't receive a password until after he or she has completed training)?
* Who is responsible for training? Is it a centralized (*e.g.*, the registrar's office) or decentralized function (*e.g.*, every department that has access to student data)?
* Consider all the options available for training and education: videotapes, workshops, documentation (both for training and for reference), and use of case studies. Some examples of training materials are included in this manual.
* Consider tailoring training for the audience involved —make it relevant for them. The needs and issues for faculty are very different from those for front-line staff in the registrar's office.
* What steps do you take to provide ongoing training and/or updates to the campus community? There will always be staff and faculty new to your campus, and others who change roles. As technology and other means of access evolve, reminders about FERPA, particularly for those who don't regularly deal with security issues, are very important.

What expectations of accountability do you have for those who have access to student data?
* Do you have any written "sign-off" of responsibility by staff? Such a document is useful to clarify expectations, set appropriate limits, and give notice of consequences if the expectations are not met. Be sure to include an expectation to report violations.
* Ensure that you tie access directly to each staff person. For example, don't structure your security access so that multiple people use the same ID/password/pass code, and actively discourage anyone from sharing their pass code to others — even on a temporary basis.
* Do you have tracking capabilities within the system — an "audit trail," particularly for maintenance? This capability will be very important when researching problems or alleged violations of security.

Do (or should) you have a FERPA policy on your campus?
* More recent amendments to FERPA removed the requirement that every institution have a policy.
* You are still required to annually notify students about FERPA. What must be included in the annual notification?
  ◆ The right to inspect and review their records (and how to do that);
  ◆ The right to seek amendments to their records (and how to do that);
  ◆ The right to consent to disclosure (with exceptions);
  ◆ The right to obtain a copy of the institution's policy (if there is one);
  ◆ The right to file a complaint.

  Other elements in your notification should include:

  ◆ Definition of "school officials" and "legitimate educational interest" (educational need to know);
  ◆ Whether it is the institution's policy to release records information without the student's written consent to another school at which the student is enrolled or seeks to enroll;

- ◆ Which items the institution defines as directory information;
- ◆ A student's option to request "no release" (non-disclosure) of directory information. You are encouraged to include the consequences of choosing this option (*e.g.*, the student's name won't appear in an institutional directory).

See a "Model Annual Notification to Students," prepared by the Family Policy Compliance Office, at www.ed.gov/policy/gen/guid/fpco/ferpa/ps-officials.html.

Students must receive notification of this information at least annually. The mechanism of distribution is not specified — therefore it could be included with registration materials, included in a student handbook, or sent via e-mail if that is a regular means for communication with your students.

Why your campus might still want to have a FERPA policy:
* It is excellent documentation for educational and training purposes with staff and faculty;
* It is excellent documentation to use when someone —particularly a student, family members, and others in the campus community — have questions about data access and security. It also provides for consistency in responding to those questions.
* It is excellent documentation to prove institutional policies in the event that a FERPA-related problem does arise — and it helps protect institutional "memory."

Are you meeting the record-keeping requirements under FERPA?

Under FERPA, when you encounter *requests for* and/or execute *releases of* personally identifiable records information, you must record:
* the date the information was released;
* to whom the information was released;
* what records were released; and
* the purpose of the request.

You do not have to keep records for releases
* to the student.
* to school officials (with the appropriate "educational need to know").
* granted with the written consent from the student.
* of directory information (assuming the student does not have a "no release"/requested non-disclosure).

Do you have appropriate institutional policies and every-day practices in place?

This is a practical encouragement for you and the appropriate people on your campus to discuss, then implement, FERPA-related policies and practices related to situations/issues that might result in FERPA violations. It is always best to be proactive in minimizing the risk of a FERPA violation by providing the training and identifying potential illegal releases of student information. This is particularly relevant with regard to the release of information to third parties.

Here are just a few examples:
* In a practical sense, how do you balance appropriate access to information with the legitimate protection of a student's privacy? Have you created procedures for people to get information they need to conduct their business, without compromising the student's privacy? For example, can someone in the business community easily confirm the attendance or degree for one of your students (assuming the student has not requested you to withhold directory information/"no release")?
* What does your institution consider to be "directory information?" The list included in the regulations is not intended to be absolute. So long as you do not include data elements that would be considered an invasion of a student's privacy, *e.g.*, religion, citizenship, grades, SSN,

etc., you may choose additional data items. Likewise, you do not have to include everything on the list of examples in the regulations. One common misconception is that students may request that an institution block the disclosure of all information about them. This is not correct and it is incumbent on you to clarify this misconception.

* What are your institution's non-disclosure ("no release") practices? Can a student have some elements suppressed (*e.g.*, a telephone number), without necessarily suppressing all directory information? How do you receive a non-disclosure ("no release") request from your students? Do they understand the ramifications of making that decision? How does a staff person know that a student has a non-disclosure request on his or her records? Is it easy to discern that within your electronic records? How does a student reverse the decision to withhold directory information?

* How does a student gain access to their record (the right to inspect and review)? Will you routinely provide a copy, if requested? Will you charge for that copy (and, if so, how much)? Do you have an expectation for how quickly you will respond to such a request?

* How does a student request an amendment to his or her record? The regulations contain a very basic protocol, which focuses on the issues of timing and notification, but does your campus have a more specific policy in this area?

* What procedures do you have in place for releasing information to the parents of dependent students? This is a common question, so you should have a protocol in place that can be consistently followed across campus. In this area, what is the student development philosophy of your institution? How do you balance the role of the parents with the desire to regard the students as independent adults? How do you ask parents to validate dependency? How do you build the student into the notification loop? Do you have "pre-waivers" by students — general (all records that the student would have access to), or specific (*e.g.*, financial information only)? Have you examined this issue at your institution?

* What do you consider to be a valid signature or authorization for release of information? A faxed signature can be considered valid — but is that in your policies? The federal *Electronic Signatures in Global and National Commerce Act*, as well as FERPA Section 99.30(d), permit the use of electronic signatures as authorization for releasing information. Again, does your institutional policy address electronic signatures?

* Do you have an established procedure to respond to subpoenas? Unless the subpoena, on its face, legally prohibits you from doing so, you must inform the student as part of the process.

* Do you routinely release results of disciplinary proceedings to alleged victims?

* How do you treat the records for deceased students? FERPA rights, and the right to privacy, legally end at death, so this is an institutional policy decision.

* Another recent amendment to FERPA permits institutions to inform the parents of a student under the age of 21 (even if he/she is not dependent) that their child has violated laws or rules related to the use of alcohol or drugs. However, you are not required to do so. Does (or should) your institution routinely do this?

These are just some of the issues you may want to address in your planning, policymaking, and implementation of procedures. This manual includes examples of training materials, solutions to potential problem situations, and a wealth of other practical information. Utilize these materials to help you and your campus identify the issues you want to address as you evaluate your institution's FERPA compliance.

In case all else fails, contact:

LeRoy Rooker, Director
Family Policy Compliance Office
U. S. Dept. of Education
400 Maryland Ave., SW

Washington, D.C. 20202-5920
(202) 260-3887 (phone)
(202) 260-9001 (fax)
E-mail: ferpa@ed.gov
Web: www.ed.gov/policy/gen/guid/fpco/index.html