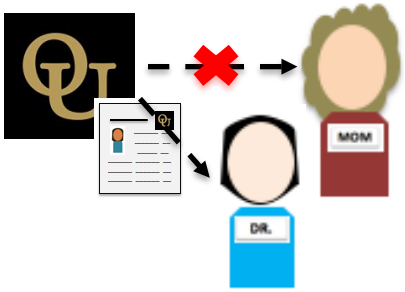
The Center for Excellence in Teaching and Learning Quick Notes presents

FERPA Guide for Faculty

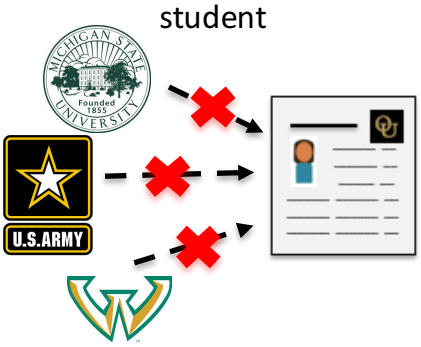
FERPA stands for the Family Educational Rights & Privacy Act of 1974.
This act has several provisions that protect a student's information:

Allows students to inspect their own education records

Prohibits the disclosure of personally identifiable information without written permission from the student



Prohibits the inspection of student records without written permission from the student



Education records are directly related to a student and maintained by an educational agency or institution or a third party acting on their behalf. They do not include your private notes that are not accessible by others and not stored in the student records. Only faculty, administrators and staff can have access to these records on a need-to-know basis.

Faculty Compliance with FERPA

- ☐ **Refraining from Discussions of Student Work with Others** Do not have discussions regarding student progress with anyone other than the student without the student's consent (including parents or guardians).
- ☐ **Writing Letters of Recommendation** Obtain written authorization from students when using educational information. This includes GPA, class standing, or class grade.
- ☐ **Securing Hard Copies of Student Work** Lock file cabinets and offices where student records are kept. When no longer needed, permanently destroy any physical or digital records that contain personally identifiable student education information.
- ☐ **Sharing Grade Information** Refrain from posting student grades by name, Grizzly ID number or any other personally identifiable number. Instead, instructors may create unique identifiers; however, the posting order must not be alphabetic. The Moodle Grades tool is a secure way to share grades with students.
- ☐ **Guard Student Information in Classroom** Do not leave graded papers unattended with student names or Grizzly ID numbers on classroom desks or tables in open view or for students to collect themselves. Do not circulate class lists that include student name, Grizzly ID number or grades as an attendance roster.

FERPA and Learning Technology

As faculty use technology to facilitate learning and foster peer collaboration, consider whether your use of technology complies with FERPA.

Using Programs and Applications Outside of the University's Learning Management System The only learning management system that Oakland University endorses is Moodle. If you plan on using other technologies outside of Moodle that could reveal students' private information, such as email addresses, have a FERPA discussion with the class and ask whether or not any student has opted out of directory information (formally through the process in the Registrar's Office). If a student indicates that they have opted out, determine another way that the student can participate in the activity.

Using Email At OU, student email addresses are included in the university's directory unless a student opts out of having their email address viewable. If using email to communicate with groups of students, use the BCC (blind carbon copy) option for listing recipients so that students do not see one another's email addresses.

Using Cloud Storage for Student Work Cloud storage options such as Google Drive and Dropbox offer class work convenience, but shouldn't be used to store students' personal information such as student ID numbers. Consult your university's tech support about secure server storage options. OU offers OakShare as a secure storage option at files.oakland.edu.

Created by the Center for Excellence in Teaching and Learning at Oakland University. Page 1 written content comes from Oakland University's Dean of Students' FERPA Guide for Faculty at oakland.edu/deanofstudents.