ACADEMIC SUPPORT RESOURCES
Office of Undergraduate Education

UNIVERSITY OF MINNESOTA
Driven to Discover®
Crookston Duluth Morris Rochester Twin Cities

FERPA Guidance Related to Online/Remote Classes and Work

FERPA is a broad law that covers all student education records. Everything in Canvas, the discussion board, assignments, and any communication to the student, is a part of a student's education record and needs to be handled safely.

As we embrace a wide range of class formats and work arrangements, there are several things to keep in mind.

Alternative Class Formats & FERPA

University tools for online meetings and educational delivery such as Zoom, Google Hangouts, and Canvas are systems you can use with private student data. To comply with FERPA when using these tools:

- Generally, you should not record classes using Zoom or similar tools if the recording captures students, unless it will only be shared within that class. (Students taking a class together are expected to be able to see each other.) Remember that names or internet IDs are typically listed as part of a person's image on Zoom and would be visible in the recording, creating a risk of disclosing private student data if the recording is shared outside of the group taking the same class. Additionally, student photos are private information, posing the same risk if the recording is shared with people outside of the class.

  - The Zoom "Spotlight" feature allows you to record only the presenter.
  - Ideally, you should have consent to record students (or others) before recording them for any purpose. Minnesota state law requires giving notice (Tennessen warning) prior to making a recording of someone.
  - If recordings are necessary for a specific purpose such as turning in an assignment, remember that recordings of students become student education records under FERPA. Save them using a university approved method (more information below) and only share them with university school officials with a need to know the private student data.
    - Use Zoom settings to manage downloads of recordings and manage other recording settings.
  - If recordings are shared with a class, that must be done carefully. See additional information about communicating with students and using student data below.
  - Using Kaltura & Canvas to record lectures is a great option that does not involve recording students.

Template language to use for notice to students:

This course will include video and audio recordings of class lectures and classroom activities. These recordings will be used for educational purposes and the instructor will make these available to students currently enrolled in [class title, number, section]. Students must seek instructor permission to share either course recordings or course content/materials. Similarly, instructors who wish to share Zoom recordings with other sections or classes must seek and document permission from students whose image or voice are in these recordings.

Template language for student consent to share recordings:

Require students to log in to a university tool such as Canvas or authenticated Google Form and affirmatively select "I agree" to language such as: I understand that Zoom recordings of this class may contain my name, photo, images, audio, chat, and other information. I give permission for [instructor] to share the Zoom recording(s) of [Class] by posting to YouTube or other publicly available platforms.

- Because the settings options on Google Hangouts/Meet are more limited, you should not record these meetings.
- Make sure you are using your university account with Zoom or Google Hangouts, and not a personal account you may have registered for with your personal email address.

- Do not require your students to be identified on social media in order to participate in class or submit assignments (e.g., sharing a Tweet or a public FaceBook post).

Do not hold meetings with your students on other technologies such as FaceTime or Skype; rely on our university-approved options in order to ensure access for students and data privacy.

Communicating with Students

- When emailing groups of students, use the Bcc line for all student email addresses. This will work for a single class of students or other groups of students. Not all students' email addresses are public.
- Contact students at their umn.edu email addresses and not alternatives. If students email you from non-umn.edu addresses, direct them to check their umn.edu account for your response.
- Calendar invites to your class (e.g., to share a Zoom link) should be marked "private" so that your class list is not disclosed via people's calendars.

Guests in Academic Classes

From a FERPA perspective, students that are enrolled together in the same class section are allowed to be aware of each other in the classroom environment, whether in person or online. Similarly, instructors or instructor-like staff such as teaching assistants have a legitimate educational interest and job need to know who is enrolled in their courses. Once you add guests and expand beyond these boundaries however, you need to take some steps to ensure you are still complying with FERPA, particularly in online formats.

Guests

First, according to university policy, students must be registered for a course in order to attend and receive credit. Students should be registered as auditors if they intend to attend the class sessions but not do homework or receive credit. (See the Grading & Transcripts policy, section C, and the Course Numbering policy.)

If someone will be attending a particular class session as a guest such as a prospective student, they should not become aware of FERPA-protected data. This means that they should not be aware of which students are enrolled in the class. In the in-person environment, this might be as simple as not having a visible class list or seating chart and using first names only when calling on students

In the online environment, there are some additional steps to take. By joining a class session on Zoom or Google Meets or similar tools, the guest can typically view the names of all of the students signed in to the same class session. The regularly enrolled students should be given advance warning of guests, and Zoom should be used so that students have the opportunity to remain private by turning their video off and renaming themselves. Students should not be penalized for remaining private when guests are present; for example they should not lose participation points.

Guests should only be added to Canvas courses in rare cases. Generally the “observer” role is recommended for guests because it avoids confusion over which students are truly enrolled and keeps more data private from the guest. Consult the Canvas Role Types resource for more information.

Guest lecturers

Guest lecturers are somewhat common at the university, and it is often easy to comply with FERPA with in-person classes. Keeping enrolled students data private is accomplished by not having a visible class list or seating chart and using first names only when calling on students. Alternatively, the guest lecturer can be asked to sign a privacy agreement that acknowledges their role as a guest lecturer and that they agree to keep private any student data obtained as a result of serving as a guest lecturer.

Adding guest lecturers to Zoom, Google Meet, or similar tools means the guest can view the names of all of the students signed in to the same class session. The regularly enrolled students should be given advance warning of guests and Zoom should be used so that students have the opportunity to remain private by turning their video off and renaming themselves. Students should not be penalized for remaining private when guests are present; for example they should not lose participation points.

Guest lecturers should only be added to Canvas courses in rare cases. Generally the “observer” role is recommended for guests because it avoids confusion over whether someone has a true instructor role and keeps more data private from the guest. Consult the Canvas Role Types resource for more information. The instructor roles in Canvas provide access to assignments and grades that is typically not appropriate for a guest. If a guest lecturer is added to Canvas, the guest lecturer should be asked to sign a privacy agreement that acknowledges their role as a guest lecturer, and that they agree to keep private any student data obtained as a result of serving as a guest lecturer.

Virtual Advising Appointments

According to FERPA, college students are responsible for their educational record and are allowed to determine whether third parties receive information about them. If the student signs a release form, the University may share information about a student’s advising record; verbal permission is not sufficient.

Because students may not have control over their external environment at the time of their virtual appointment, you should start your meetings with students as follows:

1. Let students know at the beginning of the appointment that they have a right to keep their information private, and if they need to reschedule to maintain privacy, this can be done.
2. If they cannot find a private meeting space and they choose to share specifics, ask the student to submit a consent form to share their advising information (see release form linked below).
3. If a third party is present and the student has not provided written consent to share private information, let the student and third party know you can't answer questions about the student's specifics but can answer questions about general university policies and procedures.
4. Document the conversation and outcome in APLUS.

Securing Electronic Consent for Sharing Advising Records

New Student Remote Orientation
New students completing remote orientation receive information from Orientation & Transition Experiences on how to authorize third party participation ahead of remote orientation advising meetings (see "FERPA Release Process for Remote Orientation" linked below).

Continuing Students
Continuing students can also submit consent electronically. Students can print and complete the release form (linked below), take a picture, and email it to their advisor. These forms should be routed and archived per normal office procedures upon submission. Or, students can send permission in the text of their email. These emails should also be routed and archived just as the release forms are per normal office procedures upon submission. If students send text consent, then their email must come from their umn.edu email address and must include the following elements:

> I consent to share my advising information with the person(s) described below:
> (a) first, middle and last name
> (b) month and date of birth (e.g., May 15)
> (c) relationship to student:
> (d) email address

Template Language

The following template can be used to broadly communicate this federal law to students ahead of remote appointments. For example, it can be added to Zoom waiting rooms, email signatures, APLUS appointment reminder templates, etc.:

> A student's education record at the University of Minnesota is private under the federal Family Education Rights and Privacy Act. Your advisor cannot provide your private information to a third party without your written consent. To protect your privacy during your remote advising appointment, please be in a private location or prepare to submit the consent form for anyone that will be present during the appointment.

FERPA Release Process for Remote Orientation

Student Advisor Records Release Form

Working from Home and Using Student Data

Whether you are an instructor, advisor, student services professional, or other University employee, you are likely using student data in your job. Now that you are working remotely, there might be some new considerations:

- Student data should still be stored on University-approved storage for private student data. Options include Box and Google drive (if affiliated with your umn.edu account and shared only with those that "need to know").
  - If you use a department networked drive (S: drive), this is still accessible via VPN. Avoid storing university data directly on your laptop or computer, especially if it is a personal computer.
- Use a VPN connection to safely access systems with student data. Some systems, such as APLUS, will require you to use VPN for access.
- Private student data on paper, such as unofficial transcripts, printed APAS reports, and items with student ID numbers, should be disposed of securely. Use a shredder and do not use your general recycling at home for unshredded documents.
- Wherever possible, student information should be maintained in the same systems as you would in the office. Advising notes should be entered into APLUS, final grades entered into PeopleSoft, etc.
  - Review the Maintaining Records of Student Work policy and the Grade Accountability policy for some additional guidance specific to students' graded work. Graded work and communications about grades can be sent to students' umn.edu email addresses. Make sure communications about grades are only sent to one student at a time to keep an individual student's grade private. Physical copies of graded material should be maintained according to the policy in case they are needed later.

Implementing new technology?

Departments are rapidly adopting new technology to make these unique circumstances work. Be sure not to skip important processes before implementing something new. If you are purchasing new software, check in with your local IT contact and learn about existing options the University already offers, and the appropriate steps to implement something new.

- For software that involves FERPA data, contracts should be sent to tidball@umn.edu.
- University Information Security reviews the security of vendor tools: security@umn.edu.
- The Office of General Council reviews contracts: see https://ogc.umn.edu/contracts for details.