Remote Teaching @USM:
Balancing Student Privacy and Accessibility

With the widespread move of classes and exams to remote teaching environments it is important to revisit the relevance of these activities to FERPA and other privacy laws, particularly Maryland's "all-party permission law" for recordings. At the same time, recording instructional content is often necessary in order to ensure access to students with disabilities or for those who are not able to engage in synchronous (same place, same time) digital instruction due to geography, time zone, medical issues, childcare issues, or military duties.

Stick with institutionally approved and licensed products.

Using institutionally approved and licensed products ensures that the tools have been fully vetted by your institutions' instructional technology and/or legal offices for FERPA compliance, adequate data security protocols, and accessibility. To the greatest extent possible, faculty should use these tools for all remote interactions with students and avoid, for example, having meetings with students through FaceTime, social media, or other non-institutional channels that may have questionable privacy practices or that release and share, without consent, information such as shared documents, video, and transcripts of meetings.

Institutions should review any contracts they have with third-party vendors providing information-related services to determine whether appropriate controls are in place for protecting student information that is accessed, maintained, or processed by the vendor. These contracts likely already require that digital accessibility standards have been met and express the extent to which the vendor has been put on notice of the school's and the vendor's FERPA obligations as well as any additional requirements related to confidential information and record retention. Institutions should feel free to reach out to the OAG with any concerns.

Keep challenges and barriers to access in mind.

During this time, many students face access challenges or barriers with respect to remote instruction due to differences in time zones, limited access to a computer or the internet, and familial or military duties. Because it is not dependent on being able to access class material at a precise uninterrupted time and location, asynchronous digital instruction (through learning management system content, a pre-recorded lecture, self-guided interactive learning modules), is likely to be more accessible to more individuals. Assistive technology users don't have to worry about keeping up with the pace of the rest of the class. Learners who benefit from reviewing information multiple times will be able to easily do so. Those with limited computer or internet access or parental responsibilities won't be left behind.

Students with disabilities may also experience additional and/or different challenges in this new learning environment. Approved academic accommodations must continue to be met during this time of remote instruction. In addition, students may have new access concerns due to the impact of their disability in online instruction. Please refer these students to your student disability office for additional support.

When recording for accessibility, you can protect student privacy as well.

Use of virtual classroom environments that integrate audio and video recording implicate privacy laws that are relevant for both students *and faculty* in the remote teaching environment. When you make a recording, therefore, you should observe the following best practices and considerations:

● Always provide a verbal and visual notification at the beginning of the activity notifying participants that the class is being recorded and use a visual notification of recording during the entirety of the activity so late-comers are advised as well. If a participant continues to participate after being notified the activity is being recorded, their consent is implied. Consider recording only the instructor's voice and image and limiting student participation to text-based/chat features.

● Here is a sample notification that faculty might post or present orally: *"This class is being audio-visually recorded so students who cannot attend a particular session and wish to review material can access the full content. This recording will include students' images, profile images, and spoken words, if their camera is engaged and their microphone is live. Students who do not consent to have their profile or video image recorded should keep their camera off and not use a profile image. Likewise, students who do not consent to have their voice recorded should keep their mute button activated and participate exclusively through alternative formats such as email or the chat feature." (where available).*

● Maryland's law regarding all-party consent to a recording also applies to any student who decides to make a recording from virtual classrooms. Institutions should check to see whether such student-initiated recording violates their own acceptable use or other policies. If so, institutions may wish to notify students that under institutional policy they cannot create their own recording. If student recording would not violate any campus policy, institutions may still decide to notify students that they would need to receive permission from their professor and all classmates to lawfully record this content under Maryland's all-party consent law.

● Recordings of students participating in virtual classrooms should not be stored on a faculty member's personal device. Recordings are likely to constitute "education records" under the meaning of FERPA and may also be subject to other privacy laws and institutional privacy and data retention policies. Accordingly, institutions should investigate ways to ensure that, to the greatest extent possible, recordings are maintained on servers belonging to their institution or its approved vendors. Using institutionally approved and licensed resources and platforms will ensure that the recording is stored on those systems.

Limit the use of "surveillance-based" proctoring tools. Use of "surveillance-based" proctoring, where a human proctor observes the student via webcam while taking an exam, may also implicate student privacy concerns. To the extent that surveillance- based proctoring of exams is deemed necessary, it should also be accomplished through institutionally approved and licensed vendors of proctoring products, as discussed above. Here again, institutions may wish to review their agreements with these vendors and should feel free to reach out to the OAG for support with this effort.

Be aware of special consideration for students in the EU. Lastly, any students who have relocated to the European Union may be covered by the European Union's General Data Protection Regulation, which grants additional privacy rights. In-house counsel and OAG attorneys are able to assist institutions in further assessing this risk and determining any steps institutions may be able to take to mitigate this risk.