

FAQ:



Distance Learning, Data Privacy, Records and recording

Disclaimer: This publication is for informational purposes only and is not intended as a substitute for specific legal or other professional advice. If you have specific questions about your legal or contractual rights, contact your local association or UniServ director.

1. Which laws govern the privacy of student data that may be captured or shared in the course of distance learning?

The federal Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. Similarly, §4-313 of the General Provisions Article of the Annotated Code of Maryland protects the privacy of student records, including “home address, home telephone number, biography, family, physiology, religion, academic achievement, or physical or mental ability of a student.” Both laws prohibit the disclosure of student education records/ education data to third parties without the written consent of a minor student’s parent or guardian.

Every effort should be made to keep student information confidential and out of the hands of other members of an educator’s household. Student records in an educator’s home should be stored in such a manner as to limit access to them by your family.

2. What constitutes an educational record subject to FERPA?

Educational records subject to FERPA include photos or videos that are directly related to a student, meaning the student is the focus of the video (for example, it shows them being injured, having a health emergency, contains their

personally identifiable information, or depicts an act they are disciplined for) and does not include videos where the student is incidentally captured or shows the student participating in school activities open to the public and without a specific focus on any individual. FERPA, generally, allows teachers to disclose a student’s name, photograph, and other directory information during class in which the student is enrolled without parental consent absent a specific parental request to the contrary.

It is likely that mandated recording of all classroom instruction would capture videos directly related to students and at least portions of video would qualify as an educational record, requiring prior written consent before disclosure to others.

Finally, under the Children’s Online Privacy Protection Act (COPPA), consent of a parent or guardian would be required for children under 13 to use third party platforms, such as Zoom or Google Classrooms, where that platform collects the personal information of those using it.

3. Is it a FERPA violation if parents view or listen to real-time instruction of students in my class (not recorded)?

Not necessarily. Neither federal nor state law necessarily prohibits a parent from accessing a classroom to observe their child because this information is not considered an education record or educational data. Therefore, parents may similarly observe a classroom setting that is occurring via distance learning; however, parents should notify the teacher that they are observing a lesson (s).

4. Are the data privacy requirements different for students with IEPs or special needs? What additional steps should be taken for these students?

Allowing parents to have access to real-time video or audio of students receiving special education services will not violate FERPA, but the names of students who receive these services are considered private student education records/ education data. For this reason, schools and educators should take precautions to ensure that these names are not available to other students or parents without the prior consent of parents or guardians.

If the video platform utilized to provide services could contain or reveal personally identifiable information of students, then the school system should evaluate the platform to ensure that it incorporates security measures to encrypt private data so that it may not be accessed by individuals who do not have authority to access the data. Alternatively, the schools may address privacy concerns by informing parents about the proposed services and the platform for delivery and seek parental consent.

As always, educators, especially special educators, should incorporate any additional requirements recommended by administration.

5. Can my school system require me to use security protocols that are not legally required?

Yes. School systems have the right to create and require educators to follow security protocols greater than what state or federal law requires. However, these protocols should be clearly established, consistently enforced, and available electronically for staff to review. The benefits of these additional requirements should also be balanced against ease of access for students, parents, and educators.

6. My school system requires that all lessons for distance learning be recorded so students may access them later. Can they do this? Does this raise any legal concerns?

School systems vary on this point, and we recommend following all applicable board of education policies and administrator directives you receive. Some school systems require recording so students with limited access to internet or technology may access them at a later time. Other school systems are discouraging or prohibiting educators from maintaining any recordings of their classes whatsoever. School systems have the authority to make these decisions, but the expectations should be clearly communicated and the necessary student and parent releases secured.

Specifically, with a recording of a virtual classroom, there are not only FERPA concerns, but also Maryland's wiretapping law is implicated. Specifically, it is unlawful to record someone's communications without their consent. Maryland is a two-party consent state, which requires all parties to the communication to consent to its recording. As such, recording of a virtual classroom requires the school system to secure appropriate releases from students and parents.

While real-time video of an entire classroom or group of students is not automatically subject to FERPA, video or audio recordings may be considered private student education records/ education data if they are "directly related to a student," meaning they are focused on one particular student giving a presentation. For these reasons, any recorded lessons that include students may ultimately be classified as a record protected by FERPA. Under FERPA, a parent must give written consent before a school may disclose "personally identifiable information" from student records.

7. What distance learning platform should I use?

We strongly recommend that educators not make the decision regarding which platform to utilize independently, but rather in collaboration with their department, grade-level team, and/or their administration.

8. What are the best ways to avoid issues with virtual learning?

Follow administrative directives and school policies specific to virtual learning and confirm concerns or questions in writing with school administration.

Seek consent prior to recording lessons. Teaching staff should not engage in the creation of "education records" which contain any personally identifiable information via video-recording unless consent has been acquired from every single parent/guardian/eligible student involved. The school system must be responsible for getting all such consent, and unless and until they do they should not expect educators to record their classes, and they should certainly not expect any student to appear on the video.

Valid written consent must:

- Specify the records that may be disclosed;
- State the purpose of the disclosure; and
- Identify the party or class of parties to whom the disclosure may be made.

The school system must have written consent from any and every parent/guardian/eligible student who will be involved in any such recording, even if such recording is only for the purposes of the remote learning of other students.

There may be school systems that fail and/or refuse to secure such authorizations. Although the publication of video showing students being instructed could create FERPA exposure for the school systems (FERPA does not permit a student's parent to sue a teacher personally in the event of a FERPA violation as such action may only be taken against a school), administrators and teaching staff would be indemnified so long as the directive to record is clearly mandated by the system.

In the event that releases are secured, local association representatives should demand to negotiate over the manner in which the videos are stored, length of time of storage, access to

the video, and limited use of the video (i.e. may not be used for evaluative purposes).

9. I am concerned about videos of my classes being shared on the internet or social media without my permission, or being seen by people who are not my students or their parents/guardians. What can I do to prevent this?

As is the case in your classroom, your school system may not be able to completely safeguard you from having your image or your instructional materials shared beyond their intended audience. At the same time, school systems can and should support educators' legitimate privacy concerns by prohibiting the unauthorized recording and/or dissemination of videos, images, or other data captured in the course of distance learning.

We recommend that boards of education create a written agreement for students (and/or parents/guardians, depending on age) to sign or click, containing the following language or something similar:

The following content is for educational purposes only. By accessing this material, I agree not to share this content with anyone not enrolled in the class or assisting an enrolled student. Unauthorized distribution of any distance learning content, including sharing video recordings or screenshots on the internet or social media, is strictly prohibited and could result in disciplinary action and/or the suspension of a student's access to certain distance learning materials.

School systems have an obligation to take reasonable measures to protect the privacy of students and staff. As with board of education policies prohibiting recordings in the classroom, this type of notice will make it easier for the administration to justify disciplinary action or other consequences for a student or parent/guardian who records or shares distance learning content without an educator's permission.

10. What should I do if I learn that my lessons or image have been shared without my permission?

If possible, take screenshots or document the unauthorized sharing of this content as soon as possible and provide it to your administrator. Once you have done this, contact the company where the content has been shared. Social media platforms like Facebook, Twitter, and Instagram all have ways of reporting inappropriate or abusive content so that it can be investigated and removed if it violates the company's terms of use.

School systems vary in how they respond to these incidents based on the severity of the conduct and the policies they have in place. If you believe your administration has not responded to unauthorized use of your content appropriately, contact your local association or the UniServ director for assistance.

11. Can my administrator require that I teach in real time instead of having pre-recorded lessons available for students to download?

Yes. While there is no particular guidance that has been issued by MSDE regarding the format for distance learning, the local board of education continues to possess the statutory authority to determine the method, the format, and the daily schedule of its employees so long as it complies with the work hours provided in the collective bargaining agreement.

Educators will likely not be able to provide the same type of interaction with and between students through distance learning that they can provide in a classroom, but school systems can expect educators to have ongoing interactions that include opportunities for students to ask questions and receive real-time feedback.

12. Are any notes or records that I create in the course of distance learning off limits to parents? What should I do with these records when I am done with them?

Yes. Records that you independently keep on students, which you do not share with anyone else, are considered "desk drawer notes" rather than government data and not accessible as part of a data request under the Public Information Act. When you no longer have a student in your class any associated "desk drawer notes" should be destroyed. All other information likely becomes part of the student's educational record, i.e. discipline, grades, attendance, etc.