Michael Best

August 25, 2020

Frequently Asked Questions: Privacy and Cybersecurity Issues Arising from the Virtual Learning Environment

Related Industries

Higher Education

Related Practices

Privacy & Cybersecurity

Introduction

Education technology companies are rapidly launching new and/or expanding remote learning software, and in some cases providing hardware in the form of laptops and other devices. Despite accelerated timelines for rolling out these new education technologies, legal compliance must remain a top priority. Other technology companies that are launching new education technologies must be aware that they are entering a highly regulated sector. While remote learning is critical to minimize the impact of the COVID-19 crisis on students and educational institutions, any such remote learning must be conducted in a manner that respects students' personal information and complies with the many privacy and data security laws and regulations that impact how education technology should be developed and implemented.

I. Special Considerations Arising from Use of Remote Learning or Virtual Learning Technology

a. Is Student Information Used in Online Educational Services Protected by FERPA?

It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question. The Family Educational Rights and Privacy Act (FERPA) (see 20 U.S.C. § 1232g and 34 CFR Part 99) protects personally identifiable information (PII) in students' education records from unauthorized disclosure. FERPA defines education records as "records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution" (see 34 CFR § 99.3 definition of "education record").

FERPA also defines the term PII, which includes direct identifiers (such as a student's or other family member's

name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name) (see 34 CFR § 99.3 definition of "personally identifiable information").

Schools and districts will typically need to evaluate the use of online educational services on a case-by-case basis to determine if FERPA-protected information (i.e., PII from education records) is implicated. If so, schools and districts must ensure that FERPA requirements are met (as well as the requirements of any other applicable federal, state, tribal, or local laws).

b. What are the conditions for disclosure of student education records to third party vendors?

Colleges and universities are allowed to use contractors and consultants for services -- including for online instruction -- but the contracts need to include stipulations to protect student privacy under the law. Under FERPA, education technology companies can receive student records as a service provider to the schools if the education technology company meets the school official exception, which means that the third party: (1) performs an institutional service or function for which the school would otherwise use its own employees; (2) has been determined to meet the criteria set forth in in the school's annual notification of FERPA rights for being a school official with a legitimate educational interest in the student records; (3) is under the direct control of the school regarding the use and maintenance of the student records; and (4) uses the student education records only for authorized purposes and does not re-disclose the student education records to other parties unless the education technology company has specific authorization from the school or a FERPA exception applies to the disclosure.

Most importantly, the institution should require the third party vendor to disclose all categories of information that the online provider is potentially collecting or storing if the vendor collects any data on its users, because the institution is the owner of all such information. This means that the FERPA-protected data can only be used or re-disclosed at the institution's direction. Consequently, the institution should monitor the data collection and the technology that it collects to prevent the third party vendor from creating additional student records, beyond that needed for the scope of work, which could then by inadvertently disclosed to unauthorized parties.

c. What are best practices for deployment of third party software as part of the institution's model for remote learning?

The Department of Education has advised that, in the context of virtual learning options for students, schools look for software products that apply best practices like encryption, strong identity authentication, and a statement and terms of service that explain how the vendor's use of PII from student education records complies with FERPA.

Additionally, institutions should urge the entire campus population to adopt only the software that the institution's IT department has pre-approved and selected because those contracts provide specific assurances about how the data collected can be used and shared and also restrictions about it being used for advertising or other purposes beyond the scope of the service.

II. Special Considerations Arising from the Use of Monitoring Software and Hardware

Some campuses are considering the deployment of attendance, exam, and misconduct monitoring surveillance edtech, which invariably involves authentication of the student's identity, by methods that may include facial recognition technology.

a. What are the legal implications of monitoring student attendance, student misconduct and online exams?

The information collected from students to verify identity, for purposes of recording attendance or to monitor conduct during class or exams may include PII and, thus, be protected as a student education record. For example, webcam monitoring and/or the collection of a student's facial image may implicate laws in Texas and Illinois that protect the privacy of biometric information. Each technology tool should be evaluated on a case-by-case basis to assess the exact data that is requested or needed and the accompanying agreement must be reviewed to make sure that the necessary FERPA language is included. In addition, even without regard to FERPA, the institution should adopt the best practice of providing each student with full disclosure of what data will be collected and the purpose for which it will be used, as well as obtain the student's written consent. However, having the written consent will also provide a basis for the collection under FERPA.

III. Special Considerations Arising from Live or Recorded On-Line Lectures

a. Can I take PII from my students' education records home with me?

Yes. FERPA does not prohibit teachers from taking PII from students' education records home with them as long as the teacher has a legitimate educational interest in the education records, as determined by their educational agency or institution. School officials, including teachers, who take education records home are prohibited from further disclosing the PII from the education records, except as otherwise permitted under FERPA; and, should use reasonable methods to protect the education records, and the PII in those records, from further disclosure. These protections can include access controls that are physical, technological, and administrative controls.

For example, the FERPA directory information exception would permit student records to be disclosed during classroom instruction to students who are enrolled in and attending a class, including via a virtual meeting. Thus, an education technology company could offer schools a platform for students to join a virtual classroom from home even though other household members may be able to observe such meetings and see the names of the other students attending the class. For students who cannot join a class during a live session, the same FERPA exception could apply to the students watching a recording of the class at some later time. However, individual sessions between a teacher and student, during which other student records such as grades may be discussed, should be conducted in a private location within the home.

b. Can I upload recordings of my lectures to my YouTube account which students can subscribe to and view on demand?

If the YouTube account is public and not limited to students in your classroom, then the answer is **no**. Any live or recorded classroom activity that depicts students or that allows for the identification of a student is protected under FERPA. In such situations, individuals who are not officials of the institution and are not registered for a specific class may not view class recordings or live sessions. Sharing recordings with students in the class is not a violation of FERPA and no additional student consent is required for this use of the educational record.

If a recording includes only the instructor, it is not a student record and FERPA does not limit its use. However, instructors should still include language in the syllabus regarding expectations that students not share classroom recordings with anyone not enrolled in the course.

c. Does a student have a right to record my lecture and share it with a non-institution official like a parent or a friend?

No, not if other students are identifiable in such recordings. In such cases, the syllabus or a statement from the faculty member should prohibit students' capture or copying of the recording by any means or sharing with others. This is a violation of FERPA and, while the student would not be personally liable, the institution could be cited. If such a statement is clearly made to students, and they violate it, it would become a potential violation of the institution's Code of Student Conduct.

d. If no student is identifiable in the recording of my lecture, does the student still need my written consent to share recordings?

To protect course materials from being shared, instructors should tell students that the instructor's written consent is required for them to share, in any fashion, the content of instructional materials. If such a statement is clearly made to students, and they violate it, it would become a potential violation of the Code of Student Conduct.

e. Do I need to worry about FERPA within my own online learning environment?

There are no FERPA violations in sharing classroom videos or discussions with your class. You should announce that the session will be recorded and allow students to self-select out of camera range if they so desire.

f. Can the instructor show recordings from last year's class to the current class?

Under FERPA, this situation must be treated as if the recordings were being shown to a third-party audience which requires FERPA compliance through use of consents from identifiable students or by editing out those students from the video.

g. What is the easiest way to comply with FERPA if an instructor is video-recording class sessions in which students will be asking questions/doing presentations, and the instructor wishes to share the recording with a future class?

Record only the parts of your session that show the instructor. Plan to hold specific Q&A periods during the session and when the instructor gets to one, click Pause recording.

When the instructor is ready to present again, he or she may resume recording.

While recording, instructors should not refer to students by name (de-identifying the students removes the need for a specific consent from each student depicted). If a student happens to appear on camera, their identity can be edited out or written consent can be obtained.

Videos of students giving presentations and student-generated video projects are covered by not only covered by FERPA and but also copyright (students own the copyright of their work, just as any other author/creator). Therefore, written consent under FERPA is required as well as written permission from the student to use these digital works.

Related People

Daniel Kaufman
Partner
dakaufman@michaelbest.com
T 312.836.5077

José Olivieri
jaolivieri@michaelbest.com
T 414.225.4967

Elizabeth Rogers, CIPP/US
Partner
earogers@michaelbest.com
T 512.640.3164

Elizabeth Rogers
Partner
earogers@michaelbest.com
T 512.640.3164