COLORADO
CHARTER SCHOOL INSTITUTE

Q&A: Student Safety and Privacy in Virtual Learning Environments

CSI offers this guidance to relay requirements and considerations for schools related to student safety and privacy in virtual learning environments and on videoconferencing apps. It is provided for informational purposes only and is not to be construed as legal advice or formal legal opinion on the behalf of the author or CSI. Use of this information does not create an attorney-client relationship, nor is the creation of such relationship intended by the provision of this information. This information does not constitute a formal administrative opinion on behalf of CSI. CSI recommends that each school contact its attorney to obtain legal advice with respect to any particular issue.

Internet Safety and Cybersecurity

Q: What is "internet safety"?

A: Internet safety includes "knowing about one's Internet privacy and how one's behaviors can support a healthy interaction with the use of the Internet."

Q: What is "cybersecurity"?

A: Cybersecurity is the "process of protecting information and information systems by preventing, detecting, and responding to unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Q: What is "student personally identifiable information" (Student PII)?

A: Student PII is "information that alone or in combination, personally identifies an individual student or the student's parent or family, and that is collected, maintained, generated, or inferred by a public education entity, either directly or through a school service, or by a school service contract provider or school service on-demand provider." CRS 22-16-103

Q: What laws has Colorado established relevant to internet safety/cybersecurity in K-12 education?

A: Colorado has at least three statutes relevant to internet safety/cybersecurity in our schools:

1. **Children's Internet Protection Act:** Federal law imposes certain internet safety requirements on schools that receive discounts for Internet access or internal connections through the E-Rate Program, including the adoption of an internet safety policy**.** In alignment with federal law, CRS 22-87-101 et. seq. requires districts to "adopt and implement a policy of internet safety for minors" that "will protect children from access to harmful material without compromising either the use of the internet as an educational resource or responsible adult use of internet services in such schools." CSI's Internet Safety Policy requires all CSI Schools to adopt an internet safety policy in line with C.R.S. 22-87-104.
2. **Student Data Transparency and Security Act**: CRS 22-16-101 et. seq. establishes requirements for the development of student information privacy and protection policies as well as requirements for contracts between local education providers, including CSI schools, and technology contract providers. This includes ensuring that every provider "maintain[s] a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student PII," using "administrative, technological, and physical safeguards." The law also requires schools adopt a policy for hearing complaints from parents regarding the school's compliance

with the Student Data Transparency and Security Act.

3. **Governmental Protection and Disposal of Personally Identifiable Information and Notification of Security Breach:** CRS 24-73-101 et seq. establishes requirements related to cybersecurity for all government entities, including schools. Generally speaking, compliance with FERPA and with the Student Data Transparency and Security Act also satisfies this statute. However, CRS 24-73-103(2) also establishes requirements for the disclosure of a security breach, defined as "unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information". The law requires that, when a governmental entity, including a school, becomes aware of a security breach, it must launch a prompt investigation and, where a breach is confirmed, provide timely notice to the affected individual(s).

Q: So, what policies should our school have to address internet safety and cyber security?

A: Each school should have an Internet Safety Policy (CRS 22-87-101 et. seq.), a Student Information Privacy and Protection Policy (CRS 22-16-101 et. seq.), a Parent Complaint Policy (C.R.S. 22-16-101), and a policy for investigating security breaches and notifying affected individuals (CRS 24-73-103).

Q: Our school plans to use videoconferencing to support continued staff and student engagement in remote learning environments. What should we consider when selecting a videoconferencing tool?

A: Consider products your school already uses, as many education platforms include features that can be leveraged to support distance learning. If you are looking for a new product, work with your attorney to vet prospective solutions and consider the following best practices:

- seek out products that apply encryption and strong identity authentication;
- review terms of use and privacy policies of any technical tool to be utilized and conduct technical due diligence to confirm compliance with privacy policies;
- ensure your school complies with notification requirements under FERPA (see below) and the Student Data Transparency Act (above);
- understand the different treatment of data by companies using freemium models;
- avoid requiring students to use personal accounts for access in order to ensure data stays within the infrastructure "controlled" by the school;
- be transparent with parents, students and the school community about the product selected; and
- provide staff and student/parent training on the tool selected.

Q: How can we minimize the risks associated with videoconferencing?

A: Consider the safety tools that are offered by the platform you are using. This might include:

- enabling a waiting room where participants are checked before they can enter the conference,
- controlling meeting content by blocking sound, chat, screen sharing, and participants,
- only sharing meeting links through password protected venues,
- ensuring staff recognize the account of the person trying to join the meeting, and
- having a good understanding the tool's encryption protocols.

Establish expectations for staff and student participation and a process for reporting

inappropriate online behavior.

Q: How can our school provide peace of mind to parents who do not want their student to use the camera or microphone during online learning sessions?

A: Students can disable a computer's microphone and/or camera when signing into a videoconference and still listen to the lesson.

Q: What can our school do to ensure students are accessing appropriate material while online?

A: Although school-issued technology devices that contain content filtering help to ensure that the content accessed by students is appropriate, schools cannot monitor the content a student accesses on a personal technology device. Schools should educate families and students about the importance of being safe, responsible and respectful online. In addition, school staff should review all sites used for remote learning to ensure appropriateness.

LOOKING FOR MORE?

Colorado Charter School Institute Resources

- Student Data Transparency and Security Act Overview
- Student Data Privacy and Security Implementation Guide
- Student Data Privacy and Security Webinar
- Personally Identifiable Information Policy Overview

Colorado Department of Education Resources

- Student Data Transparency and Security Act
- Data Privacy and Security
- Assessing the Security of Online Collaborative Tools

Colorado School Safety Resource Center Resources

- Internet Safety & Digital Responsibility

Other Resources

- Distance Learning and Privacy: Privacy Considerations in Selecting Distance Learning Tools
- Data Security: K-12 and Higher Education
- Cybersecurity Considerations in a COVID-19 World

FERPA

Note: This is a compilation of questions and answers provided by the U.S. Department of Education and the Colorado Attorney General's Office on the FERPA law. For additional information, consult the original sources (See "Looking for more?" below).

Q: How does FERPA fit in?

A: FERPA is the federal law (20 U.S.C. § 1232g) that protects the privacy of PII in students' education records. The law provides parents and eligible students the right to access a student's education records, the right to seek to have the records amended, and the right to protect the PII in students' education records (See Model Notification of Rights under FERPA and Model Notice for Directory Information). Schools and teachers should take precautionary measures to protect student PII in online learning environments.

Q: Can I use videoconferencing tools under FERPA and the Student Data Transparency Act?

A: Yes. Neither FERPA nor the Student Data Transparency Act prevent schools from using these types of technical tools to support providing education to students. Schools must comply with each statute's notification and consent requirements when using these tools, depending on the level of control they have over the vendor.

Q: Can school officials take student PII from their students' education records home with them?

A: Yes. So long as the school official has a legitimate educational interest in the education records, as determined by the school. School officials should use reasonable methods to protect the education records, and the PII in those records, from further disclosure.

Q: Can teachers conduct a parent-student conference at home with a spouse in the room?

A: Yes, as long as the teacher does not disclose PII from the student's education record in hearing of his or her spouse during the conversation; or moves away from his or her spouse to discuss PII from the student's education records so that the spouse does not overhear the discussion; or obtains prior consent in writing (electronic) from the parent or eligible student for the potential disclosure of PII from the student's education records to his or her spouse.

Q: Can non-students observe a virtual classroom?

A: Under FERPA, the determination of who can observe a virtual classroom, similar to an in-person classroom, is a local school decision as teachers generally do not disclose PII from a student's education record during classroom instruction. FERPA neither requires nor prohibits individuals from observing a classroom. As a best practice though, schools should discourage non-students from observing virtual classrooms in the event that PII from a student's education record is, in fact, disclosed in such virtual classrooms.

Q: Can our school disclose student's education records, or PII in those records to a videoconferencing or virtual learning software company?

A: Yes. Under the school official exception to FERPA's general consent requirement, educational agencies and institutions may disclose students' education records, or PII in those records, to a provider of such a service or application as long as the provider:

- Performs an institutional service or function for which the educational agency or institution would otherwise use its own employees;
- Has been determined to meet the criteria set forth in in the educational agency's or institution's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records or PII;
- Is under the direct control of the educational agency or institution regarding the use and maintenance of the education records or PII; and
- Uses the education records or PII only for authorized purposes and does not redisclose the education records or PII to other parties (unless the provider has specific authorization from the educational agency to do so and it is otherwise permitted by FERPA).

Schools should work with their attorneys to review information security requirements and terms of service. FERPA does not require an educational agency to enter into an agreement under the school official exception, although it is a best practice to clarify the issues of direct control and legitimate educational interest. The school's annual notification of FERPA rights includes its criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.

Q: What can providers do with the student information they collect or receive?

A: On occasion, providers may seek to use the student information they receive or collect through online educational services for other purposes than that for which they received the information, like marketing new products or services to the student, targeting individual students with directed advertisements, or selling the information to a third party. If the school or district has shared information under FERPA's school official exception, however, the provider cannot use the FERPA protected information for any other purpose than the purpose for which it was disclosed. Any PII from students' education records that the provider receives under FERPA's school official exception may only be used for the specific purpose for which it was disclosed (i.e., to perform the outsourced institutional service or function, and the school or district must have direct control over the use and maintenance of the PII by the provider receiving the PII). Further, under FERPA's school official exception, the provider may not share (or sell) FERPA-protected information, or re-use it for any other purposes, except as directed by the school or district and as permitted by FERPA. It is important to remember, however, that student information that has been properly de-identified or that is shared under the "directory information" exception, is not protected by FERPA, and thus is not subject to FERPA's use and re-disclosure limitations.

Q: Is it permissible to record classes and share the recording of the virtual classes to students who are unable to attend?

A: Yes. Assuming the video recording does not disclose PII from student education records during a virtual classroom lesson or appropriate written consent is obtained if PII from the education record, FERPA does not prohibit the teacher from making a recording of the lesson available to students enrolled in the class.

Video recordings of virtual classroom lessons qualify as "education records" protected under FERPA only if they directly relate to a student and are maintained by an educational agency or institution or by a party acting on their behalf. FERPA's nondisclosure provisions may still apply to such video recordings even if they do not qualify as "education records," if the video recording contains PII from student education records.
Some considerations for a video recording of a virtual classroom lesson that is or will be an education record include:

- Rights of access by parents and eligible students to their education records;
- In general, written consent must be obtained prior to disclosing a student's education record or PII in those records unless an exception applies; and
- Parents and eligible students have the right to seek amendment of their education records.

Q: What should we do if we record?

A: You should do the following: 1) establish data storage policies guiding teachers on where recorded classes or meetings should be stored, and how long they should be stored for, 2) ensure that recorded classes or meetings will be stored on a secure server controlled by the school. This can be a server managed by a cloud service provider that the school has a contract or account with, 3) create policy on how to notify parents and students when they will be recorded, and 4) notify students and parents of policies associated with recording and notify students and parents prior to each recording.

Questions?

Contact CSI's Legal and Policy Associate Stephanie Aragon StephanieAragon@csi.state.co.us.

LOOKING FOR MORE?

US Department of Education Resources

- FERPA and Virtual Learning During COVID-19
- FERPA and Virtual Learning Related Resources
- FERPA & Coronavirus Disease 2019 (COVID-19)
- Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices
- Protecting Student Privacy While Using Online Educational Services: Model Terms of Service
- FERPA Model Notification of Rights
- FERPA Model Notice for Directory Information

Colorado Charter School Institute Resources

- Personally Identifiable Information Policy Overview
- Working with FERPA Webinar