

Continuity of Learning: Student Data Privacy and Safety Guidelines for Educators

Revised Dec. 10, 2020

Purpose

This communication provides supervisory unions/districts (SU/SDs), public and independent schools, and educators with information and resources concerning student data privacy and practical strategies to use whenever supporting learning models with virtual/online learning components (e.g., fully remote, hybrid, etc. models).

NEW Introduction

To best manage the COVID-19 impact on students and communities, local education systems (LEAs) in Vermont are operating across a wide variety of flexible instructional models, from traditional “brick and mortar” operations, to fully online dispositions, to a nuanced hybrid combining traditional and remote approaches. According to [ISTE](#) (2020):

“[COVID-19]...has put huge new demands on school personnel, parents, technology providers and learners themselves. Before the outbreak, schools faced the challenge of managing hundreds of software applications in their ‘brick and mortar’ digital ecosystem - and of navigating equitable student participation and engagement in online learning environments. Now, our education system must consider how to structure high quality teaching and learning with technology playing a much larger role.”

-ISTE, A Learning System for Privacy, Security and Digital Citizenship Infrastructure (2020)

What is FERPA?

[FERPA](#) is a federal privacy law that applies to educational agencies, institutions and applicable programs funded by the U.S. Department of Education. It provides parents and eligible students the right:

- to access education records and seek amendment of education records;
- to provide consent to disclosure of personally identifiable information (PII) from student education records unless a FERPA exception applies;
- and to file a complaint under FERPA

Contact Information:

If you have questions or would like additional information, please contact Sigrid Olson at sigrid.olson@vermont.gov.

What is COPPA?

[COPPA](#) sets forth limited rules governing the online collection of personal information from children ages 13 and under. According to the [US Federal Trade Commission](#), “The primary goal of COPPA is to place parents in control over what information is collected from their young children online.” The Rule was designed to protect children while accounting for the dynamic nature of the Internet. COPPA imposes certain requirements on operators of websites or online services directed at children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age” ([Complying With COPPA: Frequently Asked Questions](#), 2020).

Among other stipulations, operators covered by COPPA must ([see full list of requirements here](#)):

- Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children.
- Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children.
- Provide parents access to their child's personal information to review and/or have the information deleted.

NEW What is SOPIPA?

In 2020, the Vermont Legislature passed [SOPIPA: Student’s Online Personal Information Protection Act \(S.110; Student Privacy is in Sec. 4, p. 18\)](#), enacted as 9 VSA 2443. Vermont has joined several states across the country in enacting SOPIPA legislation that originated in California. Essentially, SOPIPA ensures that entities that provide education technology solutions to schools and educators use student data for education purposes only, and do not sell information or leverage their services or platforms to target advertising to students. Education technology companies must adhere to SOPIPA regarding student data whether there is or is not a contract in place with a school or district. Currently, federal SOPIPA legislation is being pursued. To learn more about what SOPIPA legislation looks like visit [Common Sense Media](#).

UPDATED Student Privacy Considerations and Action Steps for SUs/SDs

- Consider using the [Vermont Student Privacy Alliance](#) to adopt and implement a Student Data Privacy Agreement when implementing online applications. For more information, [see Vermont Resources below](#).
- Consider how COPPA may limit student instruction using online tools that may not be appropriate for students under the age of 13 years old.
- **Consider what should or should not be recorded in an online instructional session, including:**
 - **Who initiates the recording?**
 - **If a recording includes only the instructor, it is not considered a student record and FERPA does not limit its use. If the recording**

includes students asking questions, making presentations or leading a class, and if it is possible to identify the student, then portions containing recordings of the student constitute a protected educational record and are covered by FERPA.

- What is the purpose of the recording and how will the recording be used?
 - How will video files from virtual learning that count as student records be secured?
 - Are there plans for the recordings to be publicly accessible? (e.g., is it only available through a secure LMS? Will it be available via a public space such as YouTube?)
- Consider how to limit access to the online instructional sessions by outside entities or those who are not the intended consumers of the sessions.
 - Develop protocols and training for teachers, students and families to follow during synchronous sessions.
 - Provide means to allow parents to review the personal information collected.
 - Understand how an operator/vendor will collect, use and disclose personal information from students. Possible questions that SU/SDs could ask potential operators/vendors are:
 - What types of personal information will be collected from students?
 - How will the personal information be used?
 - Will this information be used or shared for commercial purposes not related to the provision of the online services requested by the LEA?
 - Does the SU/SD have the ability to review and delete personal information collected from its students? [NOTE: If not, the SU/SD cannot consent on behalf of the parent/guardian.]
 - What measures are taken to protect the security, confidentiality and integrity of the personal information collected?
 - What are the data retention and deletion policies for children's personal information?
 - Ensure operators/vendors delete a student's personal information once the information is no longer needed for its educational purpose.
 - Document policies and procedures around the uses of websites and online services and communicate them with students, parents and any other school personnel.
 - Are students and families informed and have given consent?
 - Has language been included in any existing communications regarding the use of student images?
 - Can families/students opt out?
 - Do web-based tools have the capacity to meet the needs of students who opt-in and opt-out?
 - Make available to parents those websites and online services to which the SU/SD has provided consent on behalf of the parent concerning student data collection, as well as the direct notices from the operators/vendors.

UPDATED Student Privacy Considerations and Action Steps for Teachers

- Only use the tools that are district-approved - do not use free tools independently that are not approved by the district.
- Do not share personal information or students' personally identifiable information (PII) in online settings.
 - **When sharing a screen, ensure that no personal information is shown.**
 - **For socializing or collaboration, consider using the video features of web conferencing *with recording off.***
- Talk with students about how they can follow protocols to ensure their own safety online and protect their personal information.
- Provide explicit instruction to students about what is and is not appropriate to share in public, online settings.
- Follow protocols established by the SU/SD for all types of remote instruction sessions, both synchronous and asynchronous.
- Do not screen capture student images without their permission, and do not post images of class sessions (showing student faces) on social media.
- Abuse or neglect witnessed during a video conferencing session should be reported in accordance with existing SU/SD policy.
- Set community norms and rules around not taking screenshots or recording the session on a separate device as this may violate SU/SD behavior management policy and procedures.
- Be transparent - at the beginning of the lesson, let students know that they will be recorded and why.

Resources

Vermont Resources

The [Vermont Student Privacy Alliance](#) is a valuable resource that is available to every district in Vermont at no cost, and provides: a database searchable by district, resource or agreement; inventories digital resources; tracks contract status; houses signed contracts; allows staff to request review of resources; and creates transparency with all stakeholders around student data privacy compliance. It is a collaboration of Vermont school districts that share common concerns around student privacy. The goal of the VTSPA is to set standards of both practice and expectations around student privacy such that all parties involved have a common understanding of expectations. We strongly encourage SUs/SDs who are not already members to visit the site and take advantage of its free resources, which includes access to a standard Vermont student data privacy agreement and sample agreements from other SUs/SDs. ([Return to Student Data Privacy Considerations and Action Steps for School Districts](#))

US Department of Education Resources

[Parent and Family Digital Learning Guide from the USDOE Office of Educational Technology](#)
[Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices](#)

[FERPA and Virtual Learning](#)

[FERPA FAQ](#)

[FAQs on Photos and Videos under FERPA from the US Department of Education \(NEW\)](#)

US Federal Trade Commission Resources

[Children's Online Privacy Protection Rule \("COPPA"\)](#)

[Complying with COPPA: Frequently Asked Questions](#)

Additional Resources

[Guidance for Recording Class Sessions with TechConnect \(Confer\) Zoom](#)

[Video Conferencing Tools in the Age of Remote Learning: Privacy Considerations for New Technologies \(COSN\)](#)

[Zoom and FERPA Compliance](#)

[Zoom HIPAA Compliance Guide](#)

[Zoom Security Guide](#)

[Zoombombing Resources](#)

[Setting Up and Securing Your School's Zoom Account](#)

[Google for Education Privacy and Security Center](#)

[Set Up Google Meet for Distance Learning](#)

[Commonsense Media How to Get Kids Ready to Video Chat for Online Classes](#)

[Cisco Webex Resources for Teachers](#)