Nov./Dec. 2020

ONcall ready-to-use NEWS

Protecting student privacy during remote learning

Most students started the new school year with remote learning. While schools rushed to distance learning in the spring because of COVID-19, districts have since had a few months to implement strong privacy and security policies related to online learning. Part of the planning process for learning during the pandemic should have included plans for schools to communicate to families how they are protecting student data.

This new school year has added to the anxiety of an uncertain time. Families are worried about their student's education, health and privacy. According to a survey by the Center for Democracy and Technology that was conducted last spring, parents reported that they are only mild to moderately concerned about their children's online safety and data privacy. Even though the survey found that parents are more concerned about their children's education and progress, results showed that the more parents learned about student data privacy, the more concerned they became. *https://bit.ly/34ojztb*

The Future of Privacy Forum (FPF) and National Center for Learning Disabilities (NCLD) published "Student Privacy and Special Education: An Educator's Guide During and After COVID-19," to help schools address privacy challenges for students with disabilities during virtual learning. The guide covers how the Family Educational Rights and Privacy Act (FERPA) applies to distance learning, best practices for using videoconferencing with students, whether other family members can be present during live video lessons and how one-on-one services can be provided on live video platforms. *https://bit.ly/34lX7kk*

FERPA and virtual learning

Federal laws such as FERPA can help districts choose what new technologies to use and how to protect student privacy during remote learning.

According to the U.S. Department of Education, here are the top five things to consider about privacy and security:

1. **Look at what your school or district already uses.** Review your current solutions first, as many education platforms include features that can be leveraged to support distance learning.
2. **Identify options.** When identifying and choosing technology tools, work with your attorneys and information security specialists to vet prospective solutions against FERPA requirements using a risk-based analysis.
3. **Consider best practices.** 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 personally identifiable information (PII) from student education records complies with FERPA.
4. **Communicate.** Be transparent with parents, students and the school community. Make them aware of the risks of their children's online activity and share easy-to-understand tips to stay safe.

(Over)

For subscription information, contact WSSDA at (800) 562-8927 or (360) 493-9231.

For content questions, contact: Marcia Latta Communications Consultant (503) 580-2612.

WSSDA
Washington State School Directors' Association

5. **Ask for help.** Consult your team of experts — your attorneys, information security specialists and peers — and ask questions.

https://bit.ly/3iskMVe

Build transparency with families

Communication with families is essential to build trust and calm anxiety. Families want to know you're implementing policy measures to protect their child during school programs and activities — in person and online. Take these actions to build in control for parents:

- Share your student data privacy policy. Let parents know your guidelines for protecting student data, how class recordings will be stored and why you chose the video conferencing platform.
- Not all students will have access to a webcam or feel comfortable being on camera. Allow parents to decide if their child will participate in video conferencing and provide an alternative method for students to connect with their teachers.
- Give parents a schedule of designated times when students are able to talk with their teachers and classmates and when the webcams will be in use.
- Provide safety and privacy tips to families who lack wifi at home and must use public wifi.

Safe videoconferencing tips

Whether your teachers are using pre-recorded or live video lessons, follow these tips from the Consortium for School Networking to protect student privacy:

- Use a platform designed for use in the K-12 classroom to ensure privacy laws are followed.
- Avoid using platforms that require students to create accounts.
- Avoid recording classroom discussions with students since audio and video of a student is considered personal information.
- Store recorded video lessons in a secure place, available to limited staff members.
- Provide teachers with guidelines on keeping their video conferencing accounts secure. Determine a secure method for teachers to share web links to lessons with students.

https://bit.ly/3ndtcTY

Resources

U.S. Department of Education COVID-19: *www.ed.gov/coronavirus*
U.S. Department of Education FERPA FAQs: *https://bit.ly/34ukZCr*
U.S. Department of Health & Human Services HIPAA resources: *www.hhs.gov/hipaa*

Contributed by Erin Good, communications consultant