LEADING EDUCATION INNOVATION

Video Conferencing Tools in the Age of Remote Learning: Privacy Considerations for New Technologies

Issue Recap

Most school systems across the country have had to make a hard and fast pivot from teaching in the classroom to remote learning. With educators, technology leaders, and students sequestered in their homes, there's a pressing need to find new ways to keep students and teachers connected. The solution has often been to use video conferencing platforms.

While some online learning platforms have been designed for use in the classroom, many of the video conferencing tools now being considered for use by school systems were once reserved primarily for business teams. As such, introduction of these tools into a classroom environment needs to be handled with care.

The benefits are clear: connection and communication. For students, the ability to see and interact with their teacher on a regular basis brings with it a sense of normalcy and comfort. For teachers, the ability to reach their students allows them to continue to provide each with the attention needed to keep the learning moving forward.

However, as with most technology platforms that were not designed for use in school systems, there are questions about whether they can be used in compliance with the federal and state student data privacy laws. There are also safety questions that need to be addressed before a video conference platform can be implemented.

Start with Privacy:

Here are some key areas for school system leaders to consider:

- Are you using a platform that has been designed for use in the K-12 classroom, or that provides a special account set up by the provider specifically for K-12 school use? If not, the provider is not likely set up to be operating in compliance with applicable privacy laws.

- Even if you are using a designated school account, review the privacy policy and terms as you would for any other technology. If you need the provider to sign a data protection agreement, do so. The COVID-19 crisis does not mean cutting corners on privacy. Just the opposite. Give yourself and your parent community the comfort you both need to know that the tools you're using are appropriate for your students and compliant with the laws.

- To further protect student data privacy, avoid setting up a video conference system that requires students to create accounts. Remember that accounts for these systems are often intended only

for adults. Instead, create an enterprise account for your school system and give teachers access. Accounts should be configured such that no student user can create their own account unless the required data sharing can be done in compliance with all applicable laws and account sign-in is necessary for safety reasons. Otherwise, students should be able to join the classroom via a simple web link provided by the teacher.

Privacy Refresh

- Whether or not students create an account on the platform, remember that classroom activity is part of the education record, subject to legal protections.
- Audio containing an individual's voice is personal information, as is video containing an individual's likeness. All must be protected in accordance with federal and state law and your school system policies.
- If you permit chat functionality to be used, get clarity on how those will be transcribed and protect them accordingly. Note that "private chats" between a teacher and student are often captured as part of the full transcript and should also be protected as part of the education record.

- Determine the secure method for teachers to use when sharing web links to video sessions with students. A web link to a video session is an invitation into the classroom. It should be kept secure and confidential, never posted publicly.

- Determine if you'll permit teachers to record their video conferences. If recording is to be permitted, define and document the specific purposes. Recordings can be useful to:
    - Share with students who may have missed a lesson:
        - Remember that this can be accomplished by asking teachers to record their lessons without students present, which further minimizes the privacy risks to students;
        - Wherever possible, avoid recording classroom discussions with students;
        - Remind students and parents that such videos are for their individual educational use and are not to be shared with others.
    - Have an affirmative record of what occurred in the class for security purposes.

  Create guidelines for where the videos must be stored. Ensure that the videos are secure in transit to storage and at rest, and that they are available only to the limited personnel who might need to review them. Also create a defined retention date for the recordings.

- As with most technologies, video conferences and webcams can be vulnerable to hackers, so take advantage of configuration settings that may allow you to run access through your existing federated identity platform and establish security settings that you can manage for educators. Also provide specific guidance for teachers on keeping their video conferencing accounts secure. For example:
    - Use complex, unique passwords;
    - Utilize 2-factor authentication;

- Store passwords securely;
- Use any established VPN to ensure you are accessing your account through the school system network;
- Avoid accessing chat, recording or other tools prohibited by policy.

Educate Your Teachers:

- Taking screen grabs, recording (outside of any defined purpose), and sharing images, videos, audio files, chat transcripts or other student personal information on social media should be prohibited. In addition, it may help to remind educators that with video conferencing, they are now looking into someone's home, so be respectful of privacy even beyond what the law requires. Also ensure that teachers have a clear and specific path for escalation in the event that they see something troubling.

- Explain how teachers can control the experience for students and maintain their safety. This might include ensuring that students can't join the conference until the teacher starts the session, deactivating any private chat capabilities, preventing any automatic camera activation for participants, and taking advantage of controls that would permit teachers to turn off participant cameras (but not to turn them on).

Build in Control for Parents:

- Not all students will have webcams, not all will be comfortable on camera, and in general, it may not be advisable to require students to turn on their webcams. Consider if you will give parents the ability to opt their child out of participating in video sessions, and have alternative connection methods, such as email or phone, available for those students who need it. To further protect student privacy, configure any video platform to ensure that participant video is off by default, and require that students or parents make an affirmative choice to turn it on.

- Set up designated times during the day when video conferencing will be used. This gives students clear expectations about when they'll be able to talk with their teachers directly as well as engage with their classmates. It also gives parents clear expectations about when their children may be in a video session. (If there is a high population of essential workers - for example, first responders, health care workers, other municipal staffers, etc. - in your community, remember that parents may not be home while webcams are in use. Giving them a schedule also gives them a chance to make their own decisions about their child's participation in a video session.)

CONNECTING WITH PARENTS

If you're introducing a video conferencing system, share simple privacy information and guidance for parents, including:

- How student data privacy will be protected;
- If sessions will be recorded and if so, for what purposes and how the videos will be secured;
- Schedule for when video conference/webcams will be in use.
- Whether or not parents may opt their child out of participating and if so, how, and how the lessons will remain available to their child;
- Alternate methods for students to be able to connect with their teachers.

CoSN Checklist

Assess the Privacy:

- Is use of the product in the classroom permissible under the operator's existing terms of service and privacy policy?
- What data will be shared with the technology provider? Have you verified that student personal information collected will only be used to support your educational purposes? When will it be deleted?
- If student data – including student images and voices – will be captured, have you identified all of the applicable student data privacy laws to consider?
- How will you use the product in compliance with your FERPA, CIPA and state student data privacy law obligations?
- Are you able to configure the product in a way that does not require students to create accounts?
- If the product will be used in classrooms where children are under the age of 13, how will the operator manage its COPPA obligations?
- Is the benefit to students outweighed by any questions about data protection?

Determine the Implementation Plan:

- Do you have the bandwidth and capabilities to properly manage the implementation, with appropriate considerations for protection of student data?
- Will you permit recording of video conferences? If so, for what purpose(s)?
    - How will you ensure that the recordings are secure in transit from the educator's computer to storage?
    - Where will the recordings be stored? How will they be secured, how long will they be retained, and who will have access to them?
- Are you familiar with all the privacy and security controls available through the platform and have you determined your default configurations?

Provide Guidance to Educators:

- Have you provided guidance to educators who will be using the technology, including requirements that prohibit screen capture or sharing of images, videos, audio files or other identifiable information from or about students on social media?
- Have you provided educators with tip sheets for keeping their accounts secure?
- Have teachers been provided with written guidance on how to maintain the default privacy and security settings (or to use them if they can't be configured at the enterprise level)?
- Do teachers know what to do if they see something concerning in a home environment?
- Do you have alternate arrangements for students without webcams, internet bandwidth, other hurdles or if their parents simply prefer that they don't participate?

Build Transparency and Trust with Parents:

- Have you provided information to parents about why you're using the technology and how you're protecting student data privacy?
- Have you provided parents with a schedule for video conferencing and any ability to opt their child out of participation?

Additional Resources:

CoSN Protecting Privacy in Connected Learning Toolkit

CoSN Coronavirus EdTech Resources

U.S. Department of Education Student Privacy Policy Office/FERPA and Virtual Learning Related Resources

U. S. Department of Education/Protecting Student Data Privacy

About CoSN:

CoSN, the national association of school system technology leaders, believes that technology is an essential component of learning today, and is deeply committed to the use and distribution of technology in school systems. However, all technologies must be properly assessed for design and appropriateness in the modern classroom. Educators and companies alike must recognize and uphold their responsibilities to protect the privacy of student data.

Working together, educators and the private sector serve millions of students by providing them with the rich digital learning experiences and access needed to succeed in college, work and life. That partnership is critical to ensuring that students will have the tools necessary for success in the 21st century.

Consortium for School Networking 1325 G St, NW, Suite 420, Washington, DC 20005