Using Videoconferencing to Support Continuous Learning

Most videoconferencing (VC) applications include tools that can be used to support interactive and appropriate VC sessions. Districts should provide training for educators in the uses of these tools, especially for instruction, protecting student data privacy, and accessibility.

Other Resources

- Microsoft (Teams): Get Started with Microsoft Teams for Remote Learning
- Google (Hangout Meets): Working Remotely with GSuite
- Zoom: Best Practices for Securing Your Virtual Classroom

Recording Videoconferences

There is no federal or state policy that prohibits or requires the recording of any educational VC. Thus, the issue of whether to allow recording of VC is a local control decision, and if yes, under what circumstances recordings should be made.

It should be noted that under the Family Education Rights and Privacy Act (FERPA), when educators record students’ faces, names, and other identifiable information, that video or audio recording becomes an educational record.

If recording is allowed by the district, the decision to do so should be guided by the business case for why a particular recording may be needed (e.g., for re-use with another class or group of students). And if recordings are made, districts should provide guidance about the retention policies for such recordings. As with other electronic resources, the Secretary of State’s document retention guidance should guide those policies and procedures.

Permission to Record

Before any recording is made, the meeting host should ensure that permission has been obtained in writing from the parents of any student who will be heard or seen on camera and should announce that the session is being recorded. A district’s existing Acceptable Use Policy procedures and Student Privacy policies will likely need to be updated to fully support continuous learning (e.g., to extend existing opt-in or opt-out permission from parents already in place for recordings in school or sharing student images online).
Using Videoconferencing/Webinars for Open Public Meetings

For meetings that have an “Open Public Meeting” requirement (see attached document from State Attorney General for more information), here are a couple of best practices to consider:

- If a district is using the webinar feature (e.g., for a board meeting), require advance registration by potential attendees that requires them to identify themselves as an appropriate attendee; or
- If a district is using a meeting feature, provide publicly the name of the person or an email address to contact to obtain an invitation to the public meeting (do not post it publicly).

Student Data Privacy Considerations

The Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) requirements apply to continuous learning as well as face-to-face education. VC sessions can be encrypted by the meeting host and should be for any session in which student data (including health information) may be discussed whether the VC session is recorded or not. In addition, districts should ensure that any VC application complies with their Student Data Privacy policies and with the Children's Online Privacy Protection Act (COPPA) which requires obtaining parent permission before use with students under the age of thirteen.

Educators should be made aware of any potential student data privacy risks when using VC applications and how to mitigate issues that may arise during use. For example, when screen sharing, confidential information could be accidently shared if it is open.

Districts cannot prevent parents from taking photographs of students engaged in a VC session. However, they may want to provide guidance encouraging them to refrain from posting photographs online of students who are not their children or using the names or other information that might identify a student.

Other Resources

- U.S. Department of Education and U.S. Department of Health and Human Services joint guidance regarding the application of FERPA and HIPAA to student health records
- U.S. Department of Education:
  - FERPA and the Coronavirus Disease 2019 (COVID-19) (March 2020)
  - FERPA and Virtual Learning (March 2020)
  - Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices (February 2014)
  - FERPA and Virtual Learning during COVID-19 (Webinar)
- Chapter 29A.604 RCW: Student User Privacy Rights in Education
- Future of Privacy Forum, FERPA|Sherpa:
  - Educator’s Guide to Student Privacy
2020 Classrooms in the Cloud (Webinar)

- COVID-19 and student privacy resources, including using social media for online learning, FERPA FAQs on disclosing student health information, and tips to prevent COVID-19 cybersecurity attacks

- F3 Law's COVID-19 Updates and Alerts, including 10 Key Steps to Establish Distance Learning Amid COVID-19
- CITE's COVID-19 Resources
- CoSN's COVID-19 edtech guidance, including the new publication Video Conferencing Tools in the Age of Remote Learning: Privacy Considerations for New Technologies
- The Utah State Board of Education: Q&A on Remote Learning and Student Confidentiality

Student Safety Considerations

Student safety policies for continuous learning can often be an extension of existing face-to-face education policies. For example, many districts already discourage private meetings between one teacher and one student, and for continuous learning, may require at least two adults to be “present” when videoconferencing or conducting a phone call with only one student; either the student’s parent or guardian, or a second educator.

As always, districts are encouraged to seek advice from their own legal counsel on specific questions about the law.

Advice from a Washington Online Educator with 10 Years' Experience on Online Learning

- Establish policies about video and phone calls as well as email and text expectations.
- Parents or guardians should always know by what method their child’s teacher will communicate, email, phone calls, video.
- When emailing or texting a student, always cc: (carbon-copy) the parent or guardian.
- No 1:1 texts or chats – always groups. This applies to parents/guardians as well as students.
- Whenever possible, communicate with your class as a whole.
- Whenever possible, use district issued equipment for calls or texts.
- Student feedback/communication should be during teacher “office hours.”
- Four P’s when communicating: personal, polite, positive, and professional.
- Dress codes apply to students and staff alike.
- Concerns should be handled by administration.
Additional Guidance on Continuous Learning Communications
The expectations below of online learning providers approved by OSPI may also be helpful in thinking about communications and continuous learning.

Processes for Communicating and Issue Resolution if there is a Concern
Students are provided information about protocols for communicating with the teacher. Information that clarifies how to contact the teacher via phone, email, and/or online messaging tools is provided.

Policies and systems are in place to resolve student, school, and parent questions, complaints, and appeals. Complaint mechanisms and protocols are clearly explained and easily accessible to students in advance of need.

Teacher Training: The Social Aspects of Online Learning
Teacher training addresses the emotional and social aspects of online learning, particularly with regard to communicating with students. Online teachers are trained to identify and mitigate the ways in which the online environment can enhance or hinder the learning experience and to be sensitive to the perception of written language.

Monitoring of Communications
A program administrator (e.g., principal, department head, lead teacher, or instructional lead) uses established protocols to monitor and intervene as necessary in the quality and timeliness of teachers’ responses to students.