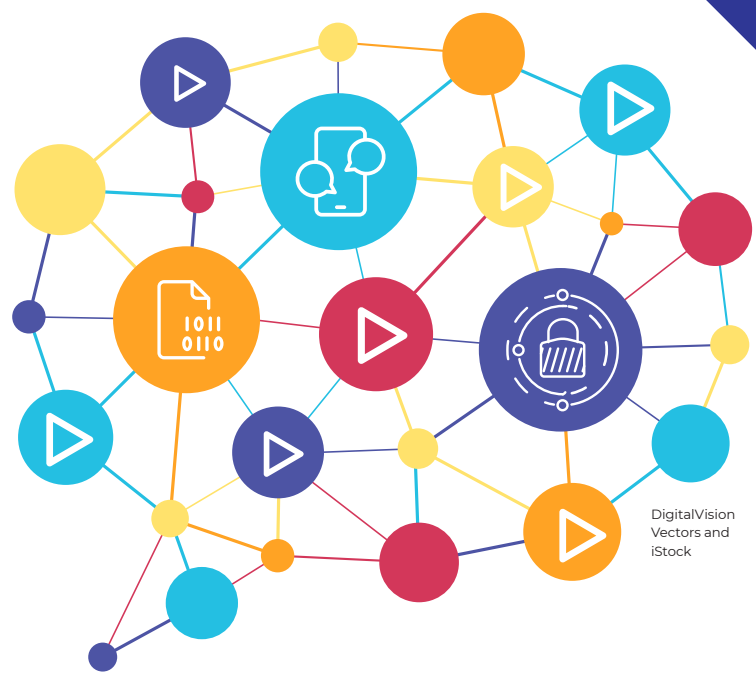
# How to Keep Students and Staff Safe on Videoconferencing

Schools across the country are turning to videoconference platforms like Zoom, Microsoft Teams, and Google Hangout to keep teachers connected to students and staff members connected to each other. In many cases, educators don't have much experience navigating the complexities and pitfalls of those platforms.

**Here's what you need to know to use videoconference platforms effectively.**



DigitalVision Vectors and iStock

## Identify a designated school or district videoconferencing platform.

Some districts already have existing relationships with online videoconference providers. In those cases, individual staff members should default to using those platforms, even if they had already set up personal accounts.

District contracts with videoconference providers typically have outlined restrictions on how and under what circumstances the company can collect and share student data. Especially for platforms like Zoom that haven't been designed with education privacy laws and norms in mind, it's important for schools to proactively advocate on behalf of their users. Several states have lists of vetted education technology products for districts and schools to consider if they don't have videoconferencing plans in place.

- **Plus, school IT departments will appreciate only having to answer questions about one designated platform.**

## Create a districtwide plan with rules for teacher-student interactions.

Each school district will have a different approach to regulating videoconferences. Experts say it's important that that approach, whatever form it takes, is written down and clearly communicated to teachers and other staff members, as well as parents.

Some questions to consider:

- How much time should teachers spend per day (or class period) talking to students via videoconference?
- Are teachers allowed to interact via videoconference with individual students?
- Are teachers allowed to, or required to, record videoconferences with their classes? With individual students?
- If yes to the above question, are they required to tell students and parents ahead of time, or secure written permission?
- How should teachers communicate with parents about expectations for their students during videoconferences?
- How should teachers dress during videoconferences with students? With colleagues?

## Be extra careful when recording students and collecting their information.

Students should be creating as few new accounts with their information—name, email address, age, address, etc.—as possible. Students should be advised to avoid using their full name on the display for a videoconference session. And schools should give parents and students ample opportunity to opt-out of being on camera or providing identifying information.

Teachers concerned about privacy may choose to only record class sessions in which students' audio and video are turned off. They can then create separate videoconference sessions that aren't recorded for students to interact after a recorded lecture.

## Take precautions against hacks and breaches.

The **"Zoombombing"** phenomenon has schools on edge about the possibility of students being exposed to inappropriate and disruptive content during class. School staff and board meetings have also been targeted.

Here are some steps to take to minimize that risk:

- Avoid sharing virtual meeting links on public platforms like social media.
- Require a password for users to enter a meeting. Change that password as frequently as feasible.
- If you're the host, be ready to disable a user's audio or video, or kick them out of the meeting entirely if they're causing a problem.
- Choose the "invite-only" option for virtual meetings when possible. Once everyone who's invited has joined the meeting, use the "lock" function to keep uninvited guests out.
- Disable private chat functions to prevent individual users (like students) from branching off into separate conversations during the virtual meeting.

- **If you do get Zoombombed or hacked, focus first on kicking the person out or even shutting down the meeting temporarily if necessary. Once that's done, notify your school or district technology team, and get back to your students or colleagues to discuss what happened.**

- **You can also report videoconferencing hack incidents to the FBI's Internet Crime Complaint Center at ic3.gov.**

## Use some simple strategies to improve the experience for everyone.

Videoconference meetings can be chaotic, especially when they involve large groups of people.

- Participants should mute their audio if they're not talking. This will minimize unwanted feedback and noise pollution from people's home background noise.
- Choose the view that suits you: A gallery of all the participants, or one person's face at a time. If you prefer the latter, pin the host of the meeting (the teacher or the principal).
- Use earbuds with a microphone to improve your audio.
- Turn off the video if you need to for any reason. For instance, on an iPhone, you can swipe right on Zoom to automatically turn your video off without pressing a button.
- Explore the other features of your videoconference platform. For instance, Zoom has tools for sharing a whiteboard and offering nonverbal feedback (like raising your hand).

SOURCES: Linnette Attai, CEO of PlayWell; Cheri Kiesecker, co-chair of the Coalition for Student Privacy; the Federal Bureau of Investigation; the Berkeley Information Security Office

EducationWeek