

The following document is part of collection of resources created by the B.C. School Counsellors Association.

The purpose of providing this resource is to ensure school counsellors offer an effective, safe and secure service, while minimizing risk and protecting the students and families we support.

The <u>USE</u> of this document (formatting&content or content only) should <u>ONLY OCCUR AFTER</u> a professional <u>COLLABORATIVE</u> <u>DISCUSSION</u> and <u>CONSULTATION</u> with your administrator.

Additionally, it important to ensure the *integration* of any of the recommendations/suggestions contained in this document be <u>compliant with School District guidelines & policies</u> regarding, security, privacy and the use of approved technologies.

All rights and permissions for use of this document, whole and in part, are granted to the end user.

Collaboration is a process not a destination!

## **Securing your Video Conferencing Experience**

BC School Counsellors

## CONSIDERATIONS FOR THE VIRTUAL SCHOOL COUNSELLOR

Leverage Your Software Settings. There are a number of settings in every platform that can help increase security for your meeting. Enable passwords for your meetings, turn off screen sharing and recording functions for attendees, and mute attendees on joining. These tools will help ensure that only invited attendees join the meeting and that an attendee can't take over your meeting with their screen without your permission.



**Remove Users.** You can remove a user from your virtual room. You shouldn't have to if you've secured your account, but know that this is available to you. Manage participants within settings of the platform. Utilize the features that allow you to block and remove participants from current and future meetings. If the platform you are using does not have these features, search for another platform that is approved by your School District.

**Share Meeting Links Carefully.** Without controls in place, a video conferencing link may let anyone join. Don't share your video conference meeting link in public places like social media. Zoom is NOT the only platform that be "bombed" or "pranked". These people are searching for OPEN meetings and wreaking havoc and disrupting the meeting.

**Recording.** If you are considering recording a virtual meeting, you need to ensure you have secured informed consent from participants BEFORE you click record. If you record, you need to inform participants where it will be stored and who will access to the recording. Use extreme caution and be transparent with meeting participants, giving careful consideration to whether the meeting contains sensitive information. It is generally a good idea NOT to record or take screen shots of students during a virtual meeting.



## **Using Video Conferencing as Participant**

**Don't Use Chats for Private Messages.** If you're attending a meeting and want to send a private message to another attendee, be aware that when your video conference that the host may have access to the transcript of the entire chat, including private messages. **Be Aware of What Personal Information You Share.** with any public forum, assume that anything you type into a chat or say in a video

conference meeting may be recorded and you don't have control of what happens to that recording. For any meeting, ask the host to clarify who has been invited to the meeting and if the meeting is going to be recorded.





**Turn Off Video and Mute Yourself Unless Needed.** If you're attending a class or meeting and you don't need video or audio, mute yourself and turn off your video. This prevents video conferencing from inadvertently recording conversations in your home or exposing information you might not want it to.

