

Increasing Safety in a Remote Learning World Guidelines



SAFER
SCHOOLS
TOGETHER

Table of Contents

Building Safe and Respectful Remote Learning Environments	2
Key Messages and Considerations.....	2
Synchronous Learning Platforms	3
General Guidelines for the Administration of Virtual Meeting Spaces	3
General Guidelines for Privacy Compliance	4
Considerations for Instructing and Learning via Synchronous Technology Platforms.....	5
Considerations for recording in the event of mis- or abusive behaviour.....	6
Other Security Notes:	6
Remote Access Trojans	6
Key messaging should include:.....	6
Resources	7
Administrator Guides:	7
Bombing Prevention:	7
Other:	7

Building Safe and Respectful Remote Learning Environments

As schools throughout BC work to deliver meaningful and engaging remote learning environments, considerations for maintaining student safe and respectful digital classroom spaces are paramount. Teachers and school administrators take great care to ensure their physical spaces encourage positive behaviour and discourage inappropriate behaviour. It is imperative that we consider our digital spaces in this same manner.

The intention of this document is to provide administrators, teachers, and parents with resources and suggestions for establishing the safest possible digital learning environments. Privacy, security, and lowest risk configurations for some of the common virtual meeting platforms are discussed.

Key Messages and Considerations

Teachers are the backbone of the British Columbia education system. We recognize the invaluable nature of relationship and that students' motivation for learning is affected by interpersonal interactions. When learning is facilitated remotely, students still seek to have their social and emotional needs met. They will continue to seek validation and attention from others, still look for opportunities to have fun, tell jokes, and find acceptance among their peers and trusted adults. Students' needs have not, and will not, change as a result of our "doing school differently." Those students who sought negative attention in the physical classroom are likely to seek similar opportunities in an online medium.

Some risk of student misbehaviour in any given environment can never be eliminated. This is as true within our physical structures as it is within digital settings. In the midst of the global pandemic, we seek to maintain the highest standards of educating within safe and respectful digital learning environments. There are a variety of things we can do to reduce students' opportunity for misbehaving online while using technologies to further facilitate and encourage socially connected learning activities.

All community stakeholders play a vital role in making decisions consistent with safe learning environments. Students are encouraged to be diligent in self-regulating behaviour and vigilant in reporting concerning behaviours of others. Parents are asked to have conversations with their children. Recognize that movement to a remote learning model may present challenges and encourage children to generatively offer suggestions to enhance their learning environment—that is, become a part of the solution. Teachers and administrators are expected to make decisions about protocols and best practices within their communities in consideration of local needs, resources and opportunities

It is important to remind students that the school’s code of conduct applies to the remote learning environment, and that online learning sessions are private – it is expected that no content from these sessions will be documented without consent or distributed online outside of the session, and that no third-party capture or social sharing of the sessions will occur.

In the same way that teaching and learning styles and needs are personal, there is not a “one size fits all” solution for remote learning that can work for all school districts/authorities within British Columbia. Comparing remote learning approaches between schools is not beneficial, nor is it advised. Students will flourish most where we contextualize approaches to teaching and learning, and consider the needs of the entire school community.

We are better together.

Synchronous Learning Platforms

Synchronous learning platforms facilitate real-time interaction and co-construction of conceptual meaning-making. Learning together, having the opportunity to ask questions, refine thinking, and deepen relationship has a positive effect on a learner’s motivation. For this reason, schools are finding vendors and software solutions to meet the need for synchronous learning engagements.

In BC, most schools are choosing between three dominant synchronous virtual meeting tool providers: Zoom, Microsoft Teams (Office 365), and Google Classroom (Google Suite for Education). Each platform provides audio and video integration, chat, screen and file sharing. Differences between the platforms centre on user experience and interface design, technical administration requirements (simplicity), and feature sets or options within the virtual meeting environment.

Without considering any specific platform, schools should consider these general guidelines for increasing the safety of all students within virtual meeting spaces. Enabling or disabling certain settings within virtual meeting spaces can limit opportunities for inappropriate behaviour.

General Guidelines for the Administration of Virtual Meeting Spaces

Each software platform provider allows for the configuration of additional security measures. While the vendors use varying titles and language for the features, the majority of security settings exist in each platform. Platforms differ in how and where those features are enabled or disabled. Some features can be controlled at the administrative level, meaning they would be set at the district or school level and locked in place, while others can be modified by the teacher or meeting host directly. The following table provides a basic overview of features and the default level of user control. Note that where a user has control of a feature (denoted by a ‘Y’ without asterisk) it is possible for administration to supersede and specify feature settings.

Setting Considerations:	CONFIGURABLE IN		
	Zoom	Teams	Meet
✓ Consider only allowing users to join meetings with their School/district accounts.	Y*	Y*	Y*
✓ Password protect class meetings and use Lobby feature.	Y	Y*	N
✓ Disable the ability for students to join the meeting before the teacher is there.	Y	Y*	Y*
✓ Do not share meeting connection details (URL) beyond the intended audience.	UB	UB	UB
✓ Disable participant file sharing in chat. (Use your school LMS for file sharing.) This setting will stop participants from sharing inappropriate images, etc. to the larger audience.	Y	N	N
✓ Disable “private” chat functionality so that students cannot DM one another within the meeting platform.	Y	Y*	N
✓ Disable participant Chat to everyone and allow messaging to teacher only.	Y	N	N
✓ Disable participant screen sharing as a default setting. Teachers can enable sharing as it is required during a class meeting.	Y	Y	N
✓ “Lock” the meeting once class is in session. This setting will stop additional participants from entering.	Y	N	N

Key: Y – configurable by user | Y* - configurable by admin only
 N – not configurable | UB – User Behaviour

General Guidelines for Privacy Compliance

- ✓ Do not use Cloud recordings. If a session must be recorded, record to local storage. Remember that these platform recording tools will record all conversation, video and audio, not only the teacher’s presentation.
 - If teachers are looking to record their presentation for later viewing by absent students, etc., consider alternate recording tools (such as Open Broadcaster Software “OBS”).
- ✓ Do not post screen shots or recordings of class gatherings on public sites (social media, etc.). Personal likeness associated with school attended is private information.
- ✓ Note that chat messages and file shares are stored on the platform provider’s servers. Private information should not be communicated through these channels.

- ✓ Content created on platform Whiteboards are stored for some time on the platform provider's server.
- ✓ Disable settings which allow participants to record the session.

Considerations for Instructing and Learning via Synchronous Technology Platforms

Teaching and engaging in synchronous learning opportunities remotely often incorporates the use of real-time streaming video, audio, and other interactive technology elements. To create the safest learning environments and reduce technical problems, teachers and participants should consider:

- ✓ Elements in the background of their video feed.
 - Best practice: orient your teaching/learning station near a solid wall as your background. Use a wall free of photos, windows, and posters.
 - Do not showcase your bedroom as a backdrop or enable your video feed while sitting on your bed, in the bathroom, etc.
 - Be sure that family members are not viewable walking around in the background.
 - Remember that you can turn your video off at any time
- ✓ Finding a quiet space. Conversations taking place in the background can be distracting and inappropriate for transmission to students, peers, or teachers.
- ✓ Where possible, hard wire to an internet modem. Relying on wireless connections is less stable and offers slower transmission speeds. Wireless connections are affected by microwaves and you may lose connection when someone decides to make some popcorn...
- ✓ Lighting. A well-lit room reduces screen-time eye fatigue and allows for clearer video.
- ✓ Video and audio use are a privilege.
 - Teachers are reminded that classroom management techniques can and should be applied to any online medium. Synchronous virtual meeting hosts must be familiar with the controls available for removing participants, disabling video, audio, chat, screen sharing, whiteboards, etc.
- ✓ Be prepared for possible technical glitches.
 - Don't panic.
 - Before you begin an online instruction session, get into the habit of rebooting your computer. This frees up many of your computer's resources which can then be allocated to the virtual meeting software.
 - Minimize the number of applications you have open.
 - Know that virtual platforms have programming which monitors the health of your connection and will try re-establishing your connection if it is dropped.
 - If your session does not reconnect, open a web browser and check to see if you still have internet by performing a Google search

Considerations for recording in the event of mis- or abusive behaviour

- ✓ Set chat logs to be saved automatically.
- ✓ Ensure that teachers know how to take screen shots.
- ✓ Ensure that teachers know how to make screen recordings using third party tools.
- ✓ Ensure that teachers know how to remove a participant from a meeting and use all security controls specific to the platform being used

Other Security Notes:

Remote Access Trojans

With the increased engagement in synchronous learning platforms, more students and families have webcam and microphone connected devices. Remote Access Trojans (RATs), which are programs that allow remote control of your device – including connected cameras and microphones and provide access to local files and programs, continue to be a part of the internet landscape which need to be guarded against. Schools are advised to engage in an education campaign with all community stakeholders to ensure families know how they can protect against RATs and what to do if they suspect one of their computers has been compromised.

Key messaging should include:

- ✓ Remote Access Trojans (RATs) are programs which allow remote control of your device including connected cameras and microphones and provide access to local files and programs.
- ✓ RATs are a form of malware often attached to files appearing to be legitimate. Peer-to-peer file downloads, email attachments, etc. are often used to distribute and infect target systems.
- ✓ RATs hide their processes so that they are more difficult to detect.
- ✓ Camera lenses on computers, tablets, and smartphones should be
- ✓ COVERED when not in use. Privacy screen or stickers can be used to
- ✓ cover built-in webcam devices.
- ✓ USB connected devices should be disconnected for additional security.
- ✓ Students are advised against having camera enabled devices in their bedrooms.
- ✓ If you are concerned that a system has been infected with a RAT:
 - Power down the system and remove its power source or unplug your internet connection router
 - Seek technical assistance which will usually include booting the system into safe mode, ensuring the network interface is disabled, then running malware detection software (like Malwarebytes).

Resources

Administrator Guides:

- ✓ Zoom School Administrators Guide to Rolling out Zoom
 - <https://zoom.us/docs/doc/School%20Administrators%20Guide%20to%20Rolling%20Out%20Zoom.pdf>
- ✓ Microsoft Teams Administrator's Guide
 - <https://docs.microsoft.com/en-us/microsoftteams/teams-overview>
- ✓ Google Classroom Meet Administrator's Guide
 - <https://support.google.com/edu/classroom/thread/33175776?hl=en>

Bombing Prevention:

- ✓ How to avoid Team Bombing
 - <https://regarding365.com/how-to-stop-teams-bombing-61c5beed8b27>
- ✓ How to avoid Zoom Bombing
 - <https://saferschoolstogether.com/news-events/how-to-avoid-being-zoom-bombed/>

Other:

- ✓ Remote Access Trojan Protection
 - <https://www.dnsstuff.com/remote-access-trojan-rat>