

Week 1 Theme: Work, Teach and Learn from Anywhere

**CYBER
AWARENESS
MONTH**

Tips for Safe Videoconferencing - Staff and Teachers -

With the use of audio/videoconferencing tools skyrocketing in both education and work environments, it is important to be aware of the inherent risks to security, safety and privacy if used inappropriately or with insufficient safety and security measures in place. As with any technology solution, it is important to follow best practices.

When used effectively, videoconferencing is a valuable tool in aiding learning instruction and work collaboration.

Please ensure you follow your school boards policies and procedures surrounding Synchronous Learning.

Selecting a Videoconferencing Tool

There are many different videoconferencing tools available on the market. However, not all tools are created equal, some are more secure than others.

Most school boards have already selected preferred videoconferencing tools for working remotely and for synchronous learning. Teachers, board staff, students and parents should consult with their school and school board for more information on which videoconferencing platforms are to be used (examples include Microsoft Teams, Google Meet and Zoom).

- Only use board endorsed or sanctioned videoconferencing tools.

Preparing / Setting up the Meetings

- Follow board/school provided videoconferencing / synchronous learning guidelines.
- Follow the tool's features and best practices for securing videoconferencing sessions. Do not assume default settings are always appropriate.
- Use a unique strong password for user accounts and do not share login credentials.
- Do not use personal social media accounts to sign in (if the option is provided).
- Make meetings private or only accessible by invited participants, and do not publicly post the videoconference announcement or meeting ID.
- Enable meeting "waiting rooms" and turn on "Announce When User Enters" for all meetings
- Protect the videoconference call with a unique password/pin
- Become familiar with the tool and its security features to operate it without assistance and know how to address issues that may occur during a videoconferencing session. For example, a participant being inappropriate in a meeting and knowing how to quickly invoke a feature to resolve the issue in order to minimize the impact to other participants.
- Be aware of the surroundings from where the session will be delivered
- Teach participants about the tool's security features they have access to. For example, using a virtual background during a session to hide private visual information such as their location's background.
- Establish videoconferencing etiquette summary for participants such as muting and unmuting microphones, and how to interact with the rest of the class.