With the use of audio/video conferencing tools skyrocketing in education, it is important to be aware of the inherent risks to security, safety and privacy if used inappropriately. As with any technology solution, it is important to follow best practices.

When used effectively, video conferencing is a valuable tool in aiding learning instruction, collaboration and engaging participants.

**Participating in a Video Conference Session**

- Become familiar with board/school provided video conferencing / synchronous learning guidelines, procedures, or policies.

- Understand the rules that apply in a virtual classroom and the resulting consequences of poor or unacceptable behaviour. Follow proper video conferencing etiquette and protocols as may have been communicated by the board, school or teacher.

- Become familiar with the video conferencing tool’s features and security best practices. For example, know how to turn off/on video and mute/unmute audio on the device.

- Use a unique strong password for user accounts and do not share logins and passwords with anyone.

- Do not use personal social media accounts to sign in (if the option is provided).

- Do not share information about the video conference session, including the meeting ID and meeting password/pin.

- Use a virtual background to blur or replace the screen’s background.

- Keep the video conferencing tool on the device up to date with the latest software patches/updates.

*Created in collaboration with ECNO, participating members from OASBO ICT and the Ministry of Education for the K-12 Cyber Awareness Month 2020.*