Thème de la semaine 1: Travailler, enseigner et apprendre de n'importe où

Conseils de sécurité pour les vidéoconférences – Participants

Vu la hausse fulgurante de l'utilisation d'outils d'audioconférence et de vidéoconférence dans le milieu de l'éducation, il est important de connaître les risques pour la sécurité et la confidentialité quand ces outils sont mal utilisés. Comme pour toute solution technologique, il faut respecter les pratiques exemplaires.

Bien utilisée, la vidéoconférence est un précieux outil qui facilite l'enseignement, la collaboration et la mobilisation des participants.

Participation à une vidéoconférence

- Prenez connaissance des lignes directrices, des procédures ou des politiques que le conseil ou l'école a fournies concernant les vidéoconférences et l'apprentissage synchrone.
- Renseignez-vous sur les règles s'appliquant dans une classe virtuelle et les conséquences en cas de mauvaise conduite. Adoptez une bonne étiquette en lien avec les vidéoconférences et respectez les protocoles communiqués par le conseil, l'école ou l'enseignante ou l'enseignant, le cas échéant.
- Familiarisez-vous avec les fonctionnalités de l'outil de vidéoconférence et les pratiques exemplaires en matière de sécurité. Par exemple, apprenez à activer et à désactiver la caméra et le son de l'appareil.
- Utilisez un mot de passe robuste unique pour les comptes d'utilisateur et ne communiquez les identifiants à personne.
- N'utilisez pas de comptes personnels de médias sociaux pour vous connecter (si cette option est offerte).
- Ne transmettez pas de renseignements sur la vidéoconférence (p. ex., identifiant et mot de passe ou NIP de la réunion).
- Utilisez un faux arrière-plan pour masquer ou remplacer le décor à l'écran.
- Gardez l'outil de vidéoconférence à jour sur l'appareil en installant les mises à jour et les correctifs logiciels.

Créé en collaboration avec ECNO, les membres participants d'OASBO ICT et le ministère de l'Éducation pour le Mois de la cyber-sensibilisation M-12 2020.