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

Conseils de sécurité pour les vidéoconférences – Personnel (enseignant ou autre)

Vu la hausse fulgurante de l'utilisation d'outils d'audioconférence et de vidéoconférence dans les milieux de l'éducation et du travail, il est important de connaître les risques pour la sécurité et la confidentialité quand ces outils sont mal utilisés ou que les mesures de sécurité sont insuffisantes. Comme pour toute solution technologique, il faut respecter les pratiques exemplaires.
Bien utilisée, la vidéoconférence est un précieux outil qui facilite l'enseignement et la collaboration au travail.

Assurez-vous de respecter les politiques et procédures de votre conseil scolaire sur l'apprentissage synchrone.

Sélection d'un outil de vidéoconférence

Il existe toutes sortes d'outils de vidéoconférence. Cependant, ils ne se valent pas tous, certains étant plus sécuritaires que d'autres.
La plupart des conseils scolaires ont déjà sélectionné des outils à privilégier pour le travail à distance et l'apprentissage synchrone. Les enseignantes et enseignants, le personnel du conseil, les élèves et les parents doivent consulter leur école et leur conseil scolaire pour en savoir plus sur les plateformes de vidéoconférence à utiliser (p. ex., Microsoft Teams, Google Meet et Zoom).

- N'utilisez que des outils de vidéoconférence approuvés par le conseil.

Organisation des rencontres

- Suivez les directives du conseil ou de l'école concernant les vidéoconférences et l'apprentissage synchrone.
- Servez-vous des fonctionnalités de l'outil et de pratiques exemplaires pour sécuriser vos vidéoconférences. Ne tenez pas pour acquis que la configuration par défaut convient toujours.
- 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).
- Organisez des rencontres privées ou uniquement accessibles aux participants invités. N'annoncez pas publiquement la vidéoconférence et ne publiez pas l'identifiant de réunion.
- Activez la fonction de « salle d'attente » et d'annonce de l'arrivée des utilisateurs pour toutes les rencontres.
- Protégez la vidéoconférence au moyen d'un mot de passe ou d'un NIP unique.
- Familiarisez-vous avec l'outil et ses composantes de sécurité pour pouvoir l'utiliser sans assistance et savoir comment régler les problèmes pouvant survenir durant une vidéoconférence. Par exemple, si un participant n'agit pas comme il se doit, vous saurez quelle fonctionnalité utiliser rapidement pour résoudre le problème et réduire les répercussions sur les autres participants.
- Soyez conscient de l'environnement d'où la séance sera transmise.
- Informez les participants des fonctionnalités de sécurité de l'outil auxquelles ils ont accès, comme l'utilisation d'un faux arrière-plan durant une séance pour cacher des éléments visuels privés, comme le décor de leur chez-soi.
- Offrez aux participants un résumé de l'étiquette liée aux vidéoconférences, notamment concernant l'activation et la désactivation du micro et la façon d'interagir avec le reste de la classe.

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.