



Considérations de sécurité pour les écoles concernant l'apprentissage en ligne

Dans le but de soutenir les enseignants, le [Centre canadien de protection de l'enfance](#) (CCPE) a élaboré une liste de considérations concernant la sécurité des plateformes et des technologies ainsi que les limites professionnelles à respecter avec les élèves sur Internet. Quel que soit l'environnement dans lequel vous enseignez (hybride ou à distance), ces considérations vous aideront à prendre les précautions nécessaires en matière de sécurité en ligne.

Sécurité des plateformes numériques

Choix des programmes et des plateformes numériques

Vérifiez les options :

- Pouvez-vous fermer une session rapidement au besoin?
- Pouvez-vous limiter les renseignements personnels que les élèves partagent (noms d'utilisateur/profils, photos/vidéos)?
- Pouvez-vous mettre les participants en sourdine, contrôler l'utilisation de la caméra, contrôler les enregistrements, désactiver les fonctions de clavardage?
- Pouvez-vous réserver l'accès d'une salle à vos élèves?
- Pouvez-vous fermer complètement une session ou est-ce que les participants peuvent rester dans la salle après votre départ?

Voyez comment l'opérateur de la plateforme utilise et gère les informations :

- Quels types et quelle quantité de renseignements personnels recueille-t-on auprès des élèves pour l'ouverture d'un compte et l'utilisation de la plateforme?
- Comment l'opérateur ou le site Web procède-t-il pour recueillir, stocker et traiter les données sur ses clients et ses visiteurs? Où ces données sont-elles stockées? Restent-elles confidentielles ou peuvent-elles être communiquées ou vendues à des tiers?

Vérifiez si la plateforme convient à l'âge des élèves :

- Quels sont les autres contenus auxquels les élèves pourraient être exposés?
- S'il y a un système de vérification d'âge, qui peut utiliser la plateforme?
- La plateforme comporte-t-elle un volet social qui permettrait à d'autres personnes de communiquer avec des élèves en dehors des activités que vous offrez?

Précautions à prendre

Prévenez les accès non autorisés :

- Pouvez-vous créer des identifiants et des mots de passe uniques et forts?
- Pouvez-vous permettre aux élèves de se connecter sans avoir à diffuser publiquement des liens ou des mots de passe?

Donnez des consignes aux élèves :

- Il est bon de demander aux élèves d'utiliser un pseudonyme différent de celui qu'ils utilisent sur leurs plateformes de médias sociaux.
- Balisez l'utilisation des webcams; n'en permettez l'utilisation que lorsque cela est nécessaire.
- Interdisez aux élèves d'enregistrer ou de prendre des captures d'écran des sessions (à l'intérieur même de la plateforme ou avec une appli ou un appareil quelconque).
- Rappelez aux élèves de ne pas s'écarter du sujet et d'utiliser un langage approprié.

Limites professionnelles à respecter avec les élèves sur Internet

Communications

- Communiquez avec les élèves et les parents à des moments appropriés de la journée et par l'entremise de plateformes scolaires établies et autorisées (plutôt que par l'entremise de vos comptes personnels).
- Maintenez vos communications dans les limites des objectifs pédagogiques.
- Assurez la transparence de vos communications sous toutes leurs formes en incluant les parents dans toute correspondance.
- Assurez la transparence de vos conversations vidéo avec les élèves. Dans une conversation vidéo, tous les participants doivent se trouver dans des aires communes et des endroits passants de leur domicile (ce qui exclut les chambres à coucher et les salles de bain). Une tenue appropriée est de mise.
- Abstenez-vous d'envoyer des demandes d'amitié à des élèves ou d'en accepter venant d'eux et de mettre des J'aime sur leurs publications sur les médias sociaux.
- Exemples de communications électroniques inappropriées : envoyer des textos à caractère personnel à des élèves; utiliser un langage désinvolte et non professionnel; publier ou retransmettre des messages, des liens ou des commentaires susceptibles d'être jugés inappropriés, offensants, discriminatoires ou incompatibles avec les normes professionnelles ou déontologiques; communiquer avec des élèves par l'entremise de comptes personnels ou d'applis de médias sociaux.

Confidentialité

- Vérifiez les politiques de votre école en matière de vie privée avant de publier sur les médias sociaux ou sur un site Web quelque chose qui puisse permettre d'identifier un élève (travaux, photos numériques, etc.).
- Appliquez les restrictions voulues pour protéger le plus possible vos comptes personnels sur les médias sociaux, de sorte que les élèves n'y aient pas accès.
- Si vous demandez aux élèves de vous envoyer des photos ou des vidéos d'eux-mêmes, conservez ces images conformément à la politique de votre école et veillez à ce que les parents sachent où elles sont conservées et quand et comment elles seront supprimées.

Demandez-vous :

- Un observateur raisonnable jugerait-il que mon interaction avec les élèves et les parents est raisonnable et professionnelle? Suis-je à l'aise avec l'idée que d'autres personnes puissent voir la session?

Si vous craignez pour la sécurité d'un enfant sur Internet, faites un signalement à [Cyberaide.ca](https://www.cyberaide.ca).