OBJET

Les employées et employés des conseils scolaires utilisent de plus en plus souvent les technologies mobiles dans le cadre de leur travail quotidien. Les appareils mobiles peuvent accroître la qualité du travail et de vie du personnel, mais ils peuvent également augmenter énormément le risque de perte de données et de divulgation d'informations personnelles. Les lignes directrices suivantes visent à aider les conseils scolaires à cerner les risques associés aux appareils mobiles et à fournir des stratégies pour l'élaboration d'une procédure ou d'un règlement interne.

Survol

Lorsqu'ils travaillent au bureau ou à l'école et à l'extérieur de leur lieu de travail, les employées et employés des conseils scolaires doivent respecter la *Loi sur l'accès à l'information municipale et la protection de la vie privée*. La Loi exige que les organismes protègent la vie privée des personnes en ce qui concerne les informations personnelles qu'ils détiennent. Cette Loi est disponible sur le site Web du commissaire à l'information et à la protection de la vie privée à http://www.ipc.on.ca.

Ces lignes directrices traduisent les meilleures pratiques pour sécuriser les appareils mobiles d'un Conseil scolaire, incluant, entre autres, les ordinateurs portatifs, les clés USB, les téléphones cellulaires et les ANP, ainsi que les informations personnelles sauvegardées sur ces appareils. La responsabilité est le premier principe de la protection de la vie privée. Lorsque des informations personnelles sont confiées aux soins ou à la garde des employées et employés d'un Conseil scolaire, ces derniers sont tenus de veiller à leur protection.

Les données appartenant à un Conseil scolaire ne doivent pas être tenues à jour ou sauvegardées sur tout appareil mobile personnel.

Les principales recommandations sont les suivantes :

- Les informations personnelles, dans toute la mesure du possible, ne doivent pas être sauvegardées sur des appareils mobiles.
- Les informations personnelles, si elles sont sauvegardées sur des appareils mobiles appartenant à un Conseil scolaire, doivent être :
  - protégées par un mot de passe et/ou cryptés de façon sécuritaire.
  - une copie seulement — pas la seule instance des données.
- Les informations personnelles doivent toujours être transmises sous forme cryptée de façon sécuritaire; ils ne doivent jamais être transmis par courriel.
- Il faut toujours détruire ou effacer les informations personnelles sauvegardées sur des appareils portatifs et des supports de stockage de sorte qu'il soit impossible de récupérer les données par la suite.

Dans le but d'alléger ce texte, le «Conseil scolaire» comprend aussi les administrations scolaires.

Lignes directrices générales

Compte tenu des risques inhérents aux appareils mobiles, ceux-ci doivent toujours être considérés comme étant non sécuritaires et, par conséquent, nécessitent une protection conformément aux lignes directrices ci-dessous.

1. **Documents électroniques/Appareils mobiles** : Dans la plus grande mesure possible, il ne faut pas sauvegarder ou accéder à des informations personnelles sur des appareils mobiles. Cette règle simple permet de réduire grandement les risques.
2. **Cryptage des données** : Si des informations personnelles doivent résider sur un appareil mobile, elles doivent être cryptées. La clé de décryptage doit être entrée manuellement; cette étape ne doit pas être automatisée. Il doit exister un moyen de récupérer les données cryptées en cas de perte de la clé de décryptage. Le cryptage du disque en entier est potentiellement l'option la plus sécuritaire disponible. Comme les normes de cryptage évoluent sans cesse, les conseils scolaires doivent s'assurer que toute solution sélectionnée réponde aux normes généralement admises, en vigueur Les installations de cryptage doivent être examinées régulièrement et mises à jour selon les besoins. En cas de doute, veuillez consulter votre équipe de technologie de l'information pour obtenir de l'aide.
3. **Copies multiples des données** : Les informations personnelles ne doivent pas être sauvegardées uniquement sur des appareils mobiles. Veuillez vous assurer qu'il existe une autre copie sur un appareil plus sécuritaire, tel un serveur qui fait l'objet d'une sauvegarde périodique.
4. **Destruction des données** : Le processus normal de suppression des données sur un disque dur, une clé USB à mémoire flash, la mémoire d'un téléphone cellulaire, etc., ne permet pas de supprimer complètement les données. Il existe des outils permettant de récupérer facilement des données et même des fragments de fichiers supprimés de ces appareils. Même si les données sont cryptées, il faut les décrypter pour les utiliser. Par conséquent, il est possible qu'elles existent à notre insu, sous forme décryptée, dans un fichier temporaire pouvant être récupéré même après la suppression. Il faut donc détruire ou supprimer les données sensibles de sorte qu'il soit impossible de les récupérer ultérieurement. Les appareils mobiles et d'autres appareils électroniques contenant ou donnant accès à des informations personnelles ou confidentielles, ou qui ont déjà été utilisés pour accéder à des informations sensibles doivent être traitées pour s'assurer que toutes les données soient supprimées de façon permanente afin de prévenir leur récupération avant que ces appareils ne soient redistribués à un autre membre du personnel, éliminés à titre d'équipement de surplus ou retournés au fournisseur.
5. **Protection par mot de passe** : L'accès à un appareil mobile doit être protégé par un mot de passe fort. Veuillez consulter les lignes directrices relatives aux mots de passe du GIVP. Sur les appareils mobiles, il ne faut pas automatiser la fourniture des mots de passe ou des autres justificatifs d'identité requis pour accéder à des données sensibles (par exemple, authentification automatique pour une application ou une base de données contenant des informations sensibles ou utilisation de Microsoft Windows pour la sauvegarde de mots de passe sur ces systèmes).
6. **Stockage des mots de passe** : Les noms d'utilisateur et les mots de passe permettant l'accès à un appareil mobile ne doivent jamais être stockés en « texte en clair » (c.-à-d., non cryptés, donc faciles à lire) sur des appareils mobiles.

7. **Protection physique** : Il faut procéder avec précaution lorsqu'on utilise des appareils mobiles dans des endroits publics, des salles de réunion ou d'autres aires non protégées afin d'éviter l'accès non autorisé aux informations ou la divulgation non autorisée de telles informations sauvegardées sur l'appareil ou pouvant être accédés à partir de l'appareil.

   Il faut redoubler de prudence dans les foules, les réunions et les aires de filtrage de sécurité afin de conserver le contrôle de l'appareil. Ne le laissez pas hors de votre vue.

   - Les appareils mobiles ne doivent pas être laissés sans surveillance et, dans la mesure du possible, doivent être sécurisés ou verrouillés mécaniquement. Utilisez un câble de verrouillage doté d'une alarme sonore lorsque vous ne les utilisez pas.
   - Lorsque vous voyagez à bord d'un transporteur commercial, vous devez transporter les appareils mobiles comme une mallette, à moins d'indication contraire du transporteur.
   - Ne laissez pas les appareils mobiles contenant des informations personnelles dans votre véhicule. (S'il est absolument impossible d'éviter cette situation, verrouillez-les dans le coffre de votre voiture avant de partir et non dans le stationnement à votre arrivée ou un autre endroit où l'on peut vous observer. Si votre véhicule n'est pas muni d'un coffre, il n'est pas sécuritaire d'y laisser des appareils.)
   - Tous les appareils mobiles doivent être identifiés de façon discrète et permanente comme appartenant au Conseil scolaire et indiquer un moyen de les retourner en cas de perte.
   - Activez la fonction de verrouillage automatique de votre appareil après cinq minutes ou plus de temps mort.
   - Effectuez du travail confidentiel uniquement sur des appareils mobiles dont vous avez le contrôle. N'utilisez pas d'ordinateurs ni de réseaux publics et ne travaillez pas avec des documents personnels ou confidentiels dans des lieux publics, et n'effectuez pas ce genre de travail sur des ordinateurs qui sont partagés avec les membres de la famille.
   - Lorsque vous regardez des informations personnelles à l'écran d'un appareil mobile dans des endroits à l'extérieur du bureau, assurez-vous que personne d'autre que vous ne puisse voir l'écran. Il ne faut jamais regarder des informations personnelles à l'écran d'un appareil mobile lorsqu'on se trouve dans un endroit public.
   - Dans la mesure du possible, il faut utiliser un système de suivi et de protection des logiciels. Il peut s'agir d'un système d'inventaire pour suivre les appareils et/ou d'une solution logicielle administrée centralement qui peut forcer les mots de passe et les politiques de sécurité pour les appareils mobiles.

8. **Protection contre les virus** : Il faut installer des logiciels antivirus et anti-espion sur tout appareil mobile en mesure de les exécuter et les configurer pour qu'ils assurent une protection en temps réel. Les programmes doivent être mis à jour régulièrement à l'aide des plus récentes rustines de sécurité.

9. **Téléphones cellulaires** : Lorsqu'ils sont en transit ou travaillent à l'extérieur du bureau, les employées et employés doivent éviter d'utiliser les téléphones cellulaires pour discuter d'informations personnelles. Les personnes qui utilisent des scanneurs ou d'autres appareils peuvent facilement entendre ou intercepter les conversations sur les téléphones cellulaires.

10. **Formation ayant trait aux appareils mobiles** : Les employées et employés doivent recevoir une formation sur la bonne façon d'utiliser les appareils mobiles. La formation doit inclure les exigences en matière de sécurité et de protection de la vie privée, ainsi que les responsabilités pour assurer la protection appropriée des informations, conformément aux présentes lignes directrices générales.

11. **Perte ou vol d'un appareil mobile** : Il y a atteinte à la vie privée lorsque des informations personnelles sont recueillies, conservés, utilisés ou divulgués de façon contraire aux dispositions de la *Loi sur l'accès à l'information municipale et la protection de la vie privée*. Les cas les plus courants d'atteinte à la vie privée sont les divulgations non autorisées d'informations personnelles en contravention à l'article 32 de la Loi. Par exemple, des informations personnelles peuvent être perdus, volés (particulièrement à partir d'ordinateurs portatifs, un très bon exemple) ou divulgués par inadvertance à la suite d'une erreur humaine. Dès qu'on apprend qu'il y a eu atteinte à la vie privée, il faut prendre des mesures immédiates. Les utilisatrices et les utilisateurs doivent communiquer immédiatement avec leur coordonnatrice ou leur coordonnateur de l'accès à l'information ou consulter les procédures en cas d'atteinte à la vie privée de leur Conseil scolaire.

Références

Université du Kansas, Bureau du commissaire à l'information et à la protection de la vie privée