



OBJET

Les présentes lignes directrices traduisent les meilleures pratiques pour assurer la sécurité des informations personnelles lorsqu'on travaille à l'extérieur du bureau ou de l'école. Dans de tels cas, des documents peuvent être sortis du bureau ou créés à l'extérieur. Cela soulève des préoccupations quant à la protection de la vie privée et de la confidentialité des documents.

Survol

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 ce que les informations soient protégées et à ce qu'il n'y ait pas d'atteinte à la vie privée.

Cela s'applique aux documents et aux informations de tous les formats (documents papier, documents électroniques, photos, dessins, enregistrements, etc.).

Les employées et employés qui travaillent à l'extérieur acheminent souvent des informations et des documents par divers moyens, incluant la technologie. Notamment, la technologie a des répercussions importantes sur la façon dont les documents sont traités et la façon dont les informations personnelles et d'autres informations sont recueillies, conservés et communiqués.

Bien que cette technologie soit efficace, elle peut diminuer la confidentialité des informations transmises. Pour cette raison, le commissaire à l'information et à la protection de la vie privée propose que les institutions encouragent les employées et employés à porter une attention particulière lorsqu'ils utilisent la technologie.

Lignes directrices

Pour de plus amples détails, consulter les guides suivants que l'on retrouve dans la trousse :

1. Lignes directrices sur les procédures relatives au mot de passe
2. Lignes directrices sur la sécurisation des appareils mobiles
3. Lignes directrices techniques sur le cryptage des données
4. Points à examiner pour l'utilisation des documents électroniques au lieu des documents papier
5. Lignes directrices sur l'élimination et la redistribution du matériel de technologie de l'information
6. Protocole en cas d'atteinte à la vie privée



Recommandations

- Les technologies mobiles utilisées à l'extérieur du bureau comprennent les ordinateurs portatifs, les clés USB, les téléphones cellulaires et les ANP. Tout appareil technologique contenant des informations sensibles doit être sécurisé en tout temps.
- Les informations sensibles, dans la mesure du possible, ne doivent pas être sauvegardées sur des appareils mobiles.
- Les informations sensibles sauvegardées sur des appareils mobiles doivent être :
 - cryptés de façon sécuritaire;
 - une copie – pas la seule instance des données.
- Les informations sensibles 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.
- Les documents originaux contenant des informations sensibles ne devraient pas être sortis du lieu de travail.

Points à examiner pour la protection des documents lorsqu'on travaille à l'extérieur

- Dans la mesure du possible, le document original devrait demeurer sur place et seules des copies devraient être retirées. Les copies devraient être clairement identifiées comme telles et être déchetées lorsqu'on en a plus besoin.
- Utilisez une procédure de signature à l'arrivée/au départ avec une date de retour pour surveiller les dossiers retirés. Dans la mesure du possible, retirez uniquement les documents pertinents, un extrait ou un résumé.
- Retournez les documents dans un lieu sûr le plus rapidement possible, par exemple, à la fin d'une réunion, la fin de la journée ou la fin d'un voyage.
- Conservez toutes les copies de travail conformément au calendrier de conservation des documents de votre Conseil scolaire, ou éliminez-les de façon sécuritaire afin qu'on ne puisse pas réassembler les documents et les lire.
- Il ne faut jamais jeter des documents contenant des informations personnelles ou confidentielles dans un bac de recyclage ou une poubelle d'un client ou dans un endroit public.
- Les documents ne doivent pas être laissés sans surveillance et, dans la mesure du possible, doivent être sécurisés ou verrouillés mécaniquement.
- Les documents de tout format doivent être transportés comme une mallette lorsque vous voyagez à bord d'un transporteur commercial, à moins d'indication contraire du transporteur.
- Ne laissez pas des documents papier ou des 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 visible. Si votre véhicule n'est pas muni d'un coffre, il n'est pas sécuritaire d'y laisser des documents ou des appareils.)



- Tous les documents et 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.
- Lorsque vous regardez des informations personnelles dans des endroits à l'extérieur du bureau, assurez-vous que personne d'autre que vous ne puisse les voir.

Travail au domicile

Désignez une aire de travail sécuritaire à titre de « bureau ».

Dans la mesure du possible, le cas échéant, installez une deuxième ligne téléphonique réservée aux appels liés au travail. Cela est particulièrement important pour les employées et employés qui ont besoin d'une ligne téléphonique pour un télécopieur ou un modem. Si un répondeur ou un service de réponse est requis, les messages liés au travail ne doivent être accessibles que par l'employée ou l'employé. Il est conseillé d'avoir un appareil distinct de celui de la maison ou d'utiliser un mot de passe différent de celui de la maison pour accéder aux messages liés au travail provenant d'un service de réponse.

Les employées et les employés doivent ranger tous les documents papier et électroniques de la façon la plus sécuritaire disponible.

Téléphones cellulaires

Il faut éviter d'utiliser des téléphones cellulaires pour discuter d'informations personnelles. Les conversations sur les téléphones cellulaires peuvent facilement être entendues ou interceptées par des individus qui utilisent des scanners ou d'autres appareils.

Lorsque les employées et employés font des appels téléphoniques depuis l'extérieur du bureau, ils doivent protéger le plus possible les informations personnelles et confidentielles. Par exemple, il faut tenir compte de l'environnement physique pour s'assurer que personne n'entend une conversation téléphonique.

Références

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