ACCÈS À L'INFORMATION ET PROTECTION DE LA VIE PRIVÉE

Approuvées le 26 septembre 2009
Révisées le 27 janvier 2011
Révisées le 24 janvier 2013
Révisées le 24 mars 2017
Prochaine révision en 2020-2021

TABLE DES MATIÈRES

Les présentes directives administratives comprennent les sections suivantes :

A. GÉNÉRALITÉS

Les présentes directives administratives donnent les grandes lignes à suivre quant à la mise en œuvre des dispositions de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (appelée la *Loi* ci-après pour alléger le texte) et les responsabilités du Conseil scolaire Viamonde (le Conseil) à cet égard. Ces directives ont pour but de mettre à la disposition du public tous les renseignements généraux et personnels auxquels il a droit, qui sont sous la garde ou le contrôle du Conseil, tout en protégeant la vie privée des particuliers dont le Conseil détient des renseignements personnels.

Le Conseil a la responsabilité de protéger la confidentialité des renseignements personnels qu'il détient sur les particuliers, les élèves qui fréquentent ses écoles, les parents, tuteurs ou tutrices, les membres des conseils d'école, l'ensemble de son personnel. Il doit également s'assurer que les registres, actifs ou inactifs, sous format papier, électronique ou autre, qui contiennent des renseignements personnels sont en sécurité et protégés de toute utilisation, divulgation et destruction non autorisées par la *Loi* en prenant toutes les précautions nécessaires.

B. DÉFINITIONS

1. Renseignements personnels

Les renseignements personnels sont des renseignements consignés qui ont trait à un particulier grâce auxquels il peut être identifié (exemples : son âge, son état matrimonial ou familial, son adresse ou son numéro de téléphone à domicile, son adresse électronique personnelle, des renseignements sur ses antécédents médicaux ou professionnels, etc.).

2. Renseignements confidentiels

Les renseignements confidentiels sont des renseignements obtenus ou confiés en confidence, c'est-à-dire qui ne relèvent pas du domaine public, et qui s'adressent à un nombre restreint

de personnes qui ont besoin d'y avoir accès (exemples : les rapports présentés au Conseil en séance à huis clos, des renseignements d'ordre financier, commercial ou technique d'une institution qui ont une valeur pécuniaire, les avis juridiques, etc.).

3. Répertoire des banques de renseignements personnels

Le répertoire de banques de renseignements personnels dresse la liste des renseignements généraux et personnels détenus par le Conseil et ses écoles. Ce répertoire est mis à la disposition du public aux fins d'examen conformément à la *Loi* et donne un aperçu des services et programmes dispensés dans les écoles et les bureaux administratifs du Conseil, fournit le genre de renseignements qu'ils détiennent et des instructions sur comment faire une demande d'accès à l'information.

4. Demande d'accès à l'information

Une demande d'accès à l'information est une demande formelle en vertu de la *Loi* dans le but d'obtenir l'accès à des renseignements généraux ou personnels d'une institution (ici présent le Conseil) ou encore dans le but éventuel d'obtenir des rectifications aux renseignements personnels ou d'inclure une déclaration de désaccord au dossier détenu par le Conseil sur le particulier qui en fait la demande. Un formulaire créé à cet effet est disponible sur le site du Conseil (voir Annexe A).

5. Appel

Toute personne qui fait une demande d'accès à l'information en vertu de la *Loi* peut interjeter appel devant le Commissaire à l'information et à la protection de la vie privée de toute décision prise par le Conseil concernant sa demande.

6. Atteinte à la vie privée

Une atteinte à la vie privée survient lorsqu'il y a une violation de confidentialité qui va à l'encontre de la *Loi* au sujet de particuliers qui peuvent être identifiés lors de la collecte, l'utilisation, la divulgation, la conservation ou la destruction des renseignements personnels qui les concernent.

C. RESPONSABILITÉS

La personne responsable de la coordination de l'accès à l'information et de la protection de la vie privée, en concertation avec la direction de l'éducation, devra :

- répondre à toute demande formelle d'accès à des renseignements généraux et personnels en vertu de la *Loi*, donner suite aux plaintes concernant la vie privée conformément aux exigences de la *Loi*;
- défendre les décisions portées en appel;
- soumettre chaque année le rapport statistique au Commissaire à l'information et à la protection de la vie privée;
- préparer à l'intention du public un répertoire des banques de renseignements personnels dont le Conseil a la garde ou le contrôle;

- veiller à ce que la collecte, l'utilisation, la divulgation, la conservation et la destruction des renseignements personnels soient faites conformément à la *Loi* et aux politiques et directives administratives du Conseil qui s'y rapportent ainsi qu'aux normes qui ont été établies au sein du Conseil à cet égard;
- assurer la mise en œuvre de la politique en cas d'atteinte à la vie privée lors d'une violation de confidentialité;
- fournir un appui à l'ensemble du personnel sur toutes les questions d'accès à l'information et de protection de la vie privée et répondre à leurs questions.

Le personnel du Conseil doit :

- transmettre toute demande formelle d'accès à l'information faite en vertu de la *Loi* à la personne responsable de la coordination de la *Loi*;
- consulter cette dernière lors d'incertitude sur le bien-fondé de divulguer ou pas de l'information;
- fournir au public les renseignements généraux sur le Conseil et ses écoles lorsque cela est approprié;
- divulguer les renseignements personnels aux personnes concernées ou aux parents, tuteurs ou tutrices des élèves âgés de moins de 16 ans, conformément à la *Loi* et toute autre loi ou règlement applicable;
- respecter la politique sur l'accès à l'information et la protection de la vie privée ainsi que l'ensemble des directives administratives et procédures s'y rapportant;
- suivre les dispositions de la *Loi* visant à respecter la vie privée des particuliers et suivre les procédures visant à préserver la confidentialité des renseignements personnels qui les concernent :
    - En informant les personnes concernées de l'autorité légale permettant la collecte des renseignements personnels qui les concernent, de l'usage qui en sera fait et du nom de la personne à qui elles peuvent s'adresser si elles ont des questions sur cette collecte, utilisation ou divulgation.
    - En veillant à ce que tous les formulaires recueillant ou divulguant des renseignements personnels soient revus par la personne responsable de la coordination de l'accès à l'information et de la protection de la vie privée.
    - En veillant à ce que les renseignements personnels recueillis soient conservés au minimum un an.
    - En veillant à la protection de la confidentialité des renseignements personnels concernant les élèves qui fréquentent les écoles du Conseil, l'ensemble du personnel du Conseil, les parents, tuteurs ou tutrices des élèves, les membres des conseils d'école et les particuliers qui transigent avec le Conseil en prenant toutes les mesures de sécurité nécessaires (rangement sous clé, etc.). La confidentialité de ces renseignements doit être maintenue en tout temps par toutes les personnes qui ont accès à ceux-ci. Seuls les membres du personnel qui ont expressément besoin des renseignements personnels dans l'exercice de leurs tâches ont accès à ceux-ci.

- En respectant le droit des particuliers à :

  - avoir accès aux renseignements personnels qui les concernent ainsi qu'à des copies de ceux-ci dans les délais prescrits par la *Loi*, et ce, sous réserve d'exceptions limitées;

  - demander le retrait, la rectification des renseignements personnels qui les concernent s'ils sont erronés ou incomplets ou l'inclusion d'une déclaration de désaccord; et

  - déposer une plainte par rapport à la protection de leur vie privée.

- En signant le formulaire d'engagement sur le respect de la confidentialité des renseignements personnels et en faisant signer ledit formulaire aux tierces personnes et aux fournisseurs externes avec lesquels des renseignements personnels sont partagés.

- En communiquant avec la personne responsable de la coordination de l'accès à l'information et de la protection de la vie privée lorsqu'un programme ou un service impliquant la collecte, l'utilisation ou la divulgation de renseignements personnels est proposé ou revu.

D. VIGILANCE À L'EXTÉRIEUR DES LOCAUX DU CONSEIL

L'évolution rapide de la technologie a grandement changé la façon dont le milieu du travail fonctionne. Le Conseil fournit de l'équipement à la fine pointe aux membres élus et aux membres de son personnel afin qu'ils puissent accomplir leurs tâches où qu'ils soient, et ce, selon leurs besoins par rapport à leurs responsabilités. Cette technologie, mise à leur disposition, leur permet d'avoir accès à des renseignements et documents par divers moyens. L'usage de la technologie a des répercussions importantes sur la façon dont les documents sont traités et sur la façon dont les renseignements personnels ou confidentiels sont recueillis, utilisés, conservés et communiqués.

Bien que cette technologie soit fort utile, il peut s'ensuivre un risque sur le respect de la confidentialité des renseignements reçus et transmis. Pour cette raison, le Conseil compte sur les membres élus et son personnel pour prendre toutes les précautions nécessaires afin de protéger les renseignements personnels ou confidentiels et d'éviter toute perte ou tout vol, quel que soit l'endroit où ils sont. À l'extérieur des locaux du Conseil et des écoles, il importe que tous et toutes fassent davantage preuve de vigilance lorsqu'ils prennent connaissance, se servent ou communiquent de tels renseignements sous format papier ou par l'entremise de la technologie mise à leur disposition. Ces renseignements doivent être gardés à l'abri de tout regard indiscret en tout temps et ne doivent jamais être laissés sans surveillance, à moins d'être mis en sécurité sous clé.

Le Conseil privilégie l'accès de données contenant des renseignements personnels ou confidentiels par l'entremise de téléconnexion protégée et sécuritaire ou d'un réseau privé virtuel tel que le site du Conseil plutôt que le transport des données avec soi au moyen de documents papier, de cédéroms ou de clés USB.

La sortie de renseignements personnels ou confidentiels ou leur accès à l'extérieur du lieu de travail régulier, quel que soit leur format (papier ou électronique), doit être limité au

minimum et uniquement lorsque cela est nécessaire. Dans la mesure du possible, seulement des copies doivent être emportées et les originaux doivent rester au Conseil ou à l'école.

Les documents, sous format papier contenant de tels renseignements, ne doivent jamais être jetés dans une poubelle, un bac de recyclage ou être réutilisés comme papier pour l'imprimante, le photocopieur ou le télécopieur.

1.0 Appareils technologiques et dispositifs mobiles ou sans fil

1.1 Les appareils technologiques comprennent les ordinateurs, les télécopieurs, les numériseurs. Les dispositifs mobiles ou sans fil comprennent les ordinateurs portables, tous les appareils mobiles, les clés USB et les téléphones cellulaires ou intelligents.

1.2 Tout appareil technologique et dispositif mobile ou sans fil, ayant accès à des renseignements personnels ou confidentiels, doivent être sécurisés en tout temps contre l'accès non autorisé et avoir un mot de passe sécuritaire, dépendant de la configuration de l'appareil. Il importe de ne pas utiliser des mots de passe prévisibles comme la date de naissance, le nom de la conjointe ou du conjoint, etc. Le mot de passe doit être mémorisé et changé régulièrement et ne doit pas être partagé avec qui que ce soit. Il importe de ne jamais utiliser la fonction «Mémoriser mon mot de passe» quel que soit le système ou le site Web utilisé.

1.3 Il importe d'être vigilants lors de la transmission de tels renseignements par courriel ou autre mode de communication, en raison de leur vulnérabilité, afin d'en assurer la sécurité (par exemple, en vérifiant qu'il s'agit du bon destinataire, en indiquant qu'il s'agit de renseignements de nature confidentielle et au besoin en indiquant que ces documents ne doivent pas être retransmis ou reproduits sans permission). Il est recommandé d'échanger de préférence de tels renseignements au moyen des bases de données du Conseil ou de dossiers partagés sécurisés. Il est également recommandé d'éviter de transmettre de tels renseignements par télécopieur, à moins de ne pouvoir faire autrement et d'avoir pris les précautions ci-dessus mentionnées. La transmission par courriel de renseignements personnels de nature délicate (exemples : évaluation psychologique d'un élève ou rapport sur le renvoi d'un élève ou le congédiement d'un membre du personnel) est à éviter lorsque cela est possible. Il est recommandé de joindre au courriel un document contenant de tels renseignements en le protégeant d'un mot de passe plutôt que de le mettre directement dans l'objet ou le message du courriel.

1.4 L'usage d'appareils technologiques, dotés du courrier électronique ou de dispositifs mobiles ou sans fil, tels que les téléphones cellulaires ou intelligents, pour consulter ou échanger sur des renseignements personnels ou confidentiels, doit être évité dans les aires publiques ou ouvertes ou lors de déplacements en transport en commun, que ce soit en autobus, en métro, en train ou en avion où il existe un risque élevé d'atteinte à la vie privée. Lors de l'usage de ces appareils, il importe de s'assurer que de tels renseignements sont à l'abri de tout regard indiscret et que la conversation ne puisse être entendue autour.

1.5 Les renseignements personnels transmis doivent, autant que possible, être anonymisés en utilisant des termes voilés, les initiales de la personne, un symbole ou

un code l'identifiant plutôt que le nom au complet afin de préserver l'anonymat de la personne à laquelle les renseignements personnels se rapportent.

1.6 Aucun ordinateur portable, appareil mobile ou sans fil ou document papier contenant de tels renseignements ne doit rester sans surveillance dans un véhicule. Dans la mesure du possible, ils doivent être emportés avec soi. S'il n'y a pas moyen de faire autrement et que le véhicule utilisé n'est pas muni d'un coffre, les renseignements personnels ou confidentiels ou les appareils détenant de tels renseignements doivent être entreposés de manière à être hors de la vue des passants et sous clé.

1.7 Seuls des cédéroms et des clés USB sécurisés (avec mot de passe ou cryptés par les Services informatiques) doivent être utilisés ou emportés à l'extérieur des locaux du Conseil s'ils contiennent des renseignements personnels de nature délicate. Ils ne doivent pas être laissés sans surveillance. Ils doivent être mis en sécurité sous clé lorsqu'ils ne sont pas en usage. Une fois le travail terminé, il est recommandé d'effacer les renseignements personnels ou confidentiels des cédéroms ou des clés USB après les avoir enregistrés sur le réseau.

2.0 Ordinateurs et ordinateurs portables

2.1 Avant d'emporter un ordinateur portable du Conseil, dont le disque dur détient des données personnelles, il importe de faire une sauvegarde de ces données sur le réseau (dans un répertoire où l'accès est restreint aux personnes autorisées), dans l'éventualité que l'appareil soit perdu ou volé et qu'il faille informer les personnes dont les renseignements personnels ont été perdus ou volés.

2.2. Les documents contenant des renseignements personnels ou confidentiels ne doivent pas être enregistrés sur le disque dur d'un ordinateur ou d'un ordinateur portable personnel si l'usage de celui-ci est partagé avec d'autres membres de la famille.

2.3 L'utilisation de techniques de cryptage récentes est recommandée pour réduire le risque d'interception lors de l'usage d'un routeur sans fil à domicile (exemple : le système d'accès protégé Wi-Fi, WPA ou WPA2).

3.0 Usage d'ordinateurs publics

3.1 Lors de l'usage d'un ordinateur public, il importe d'utiliser celui d'un établissement fiable (exemple, une bibliothèque municipale). La sécurité des communications sur Internet dépend de la fiabilité de l'ordinateur utilisé.

3.2 Lors d'opérations nécessitant un accès sécurisé, il importe de ne pas oublier de fermer la session de travail une fois terminé et de sortir de l'environnement de travail Citrix et Outlook Web. La mémoire cache du navigateur doit si possible être vidée et l'historique de navigation doit être supprimé.

3.3 Seuls des fichiers Internet provenant de sources sûres doivent être téléchargés. S'il y a un doute quelconque sur ces fichiers, les télécharger sur un disque séparé tel qu'un cédérom ou une clé USB afin d'être analysés à l'aide d'un détecteur de virus.

4.0 Usage du répondeur

Si, lors d'un appel téléphonique de nature personnelle ou confidentielle, la personne qui fait l'appel tombe sur un répondeur, il importe de ne pas laisser un message détaillé, mais de simplement demander à la personne de rappeler.

5.0 Nuages informatiques

L'utilisation de nuages informatiques, pour entreposer des documents contenant des renseignements personnels, est interdite.

E. EN CAS DE PERTE OU DE VOL D'ÉQUIPEMENT

1.0 Il importe de signaler immédiatement aux Services informatiques et à votre superviseure ou superviseur immédiat (le cas échéant) la perte ou le vol de tous ces types d'appareils, qu'il s'agisse d'ordinateurs portables, de dispositifs mobiles ou sans fil afin de minimiser le risque que des renseignements personnels ou confidentiels soient compromis.

1.1 Lors du signalement de la perte ou du vol d'ordinateurs portables ou d'appareils mobiles ou sans fil appartenant au Conseil, les Services informatiques peuvent procéder immédiatement à l'élimination des données à distance pour les appareils Apple et les BlackBerry.

1.2 La détentrice ou le détenteur d'appareils mobiles ou sans fil doit programmer ceux-ci de manière à ce que les données qu'ils contiennent soient effacées après la dixième tentative infructueuse de l'entrée du mot de passe afin de bloquer l'accès non autorisé aux données. Elle ou il doit aussi signaler aux Services informatiques la perte ou le vol de l'équipement prêté par le Conseil dans les plus brefs délais.

F. MESURES À PRENDRE PAR LES SERVICES INFORMATIQUES

1.0 Tous les portables et les tablettes électroniques doivent être identifiés de façon discrète et permanente comme appartenant au Conseil avec ses coordonnées afin qu'en cas de perte ou de vol, ils puissent être retournés au Conseil.

1.1 Les dispositifs mobiles ou sans fil, les ordinateurs portables contenant des renseignements personnels ou confidentiels, en attente de retrait, doivent être conservés de façon sécuritaire. Ils doivent donc être mis dans un endroit qui ferme à clé ou au minimum, dans un endroit où l'accès est limité et contrôlé.

1.2 Les renseignements personnels ou confidentiels sauvegardés sur tout équipement excédentaire tel que des ordinateurs portables, des appareils portatifs, électroniques ou sans fil (téléphones cellulaires ou intelligents, tablettes électroniques, etc.) ou encore sur des supports de stockage doivent toujours être détruits ou complètement effacés et épurés avant que le Conseil s'en débarrasse, de sorte qu'il soit impossible de récupérer par la suite les données. Il importe de s'assurer de ne pas compromettre la vie privée d'une personne avant que le Conseil se défasse de ces appareils. Entre autres, les fichiers devront être supprimés ainsi que ceux qui se trouvent dans la corbeille. Le disque dur devra être reformaté.

G. LISTE DES ACCÈS

Le Conseil tient une liste à jour des accès accordés aux différents groupes d'employés. Ces accès sont accordés en tenant compte des responsabilités qui incombent aux membres du personnel afin qu'ils puissent accomplir leurs tâches.

Réf. : politique et directives administratives 1,15 sur l'atteinte à la vie privée

Conseil scolaire Viamonde

FORMULAIRE DE DEMANDE

En vertu de la *Loi sur l'accès à l'information municipale et la protection de la vie privée*

Note : Veuillez transmettre votre demande à Martine Pioffet, coordonnatrice de l'accès à l'information et de la protection de la vie privée, soit par courriel : pioffetm@csviamonde.ca, par télécopieur au 416 397-2047 ou par la poste à l'adresse 116, Cornelius Parkway, Toronto (Ontario) M6L 2K5, accompagnée du paiement des frais de dossier de 5 $.

Demande :	**Nom de l'institution à laquelle la demande est présentée :**
☐ Accès à des documents d'ordre général ☐ Accès à des renseignements personnels sur soi ☐ Rectification de renseignements personnels sur soi	

S'il s'agit d'une demande d'accès à des renseignements personnels sur soi ou de rectification de ceux-ci :

Nom de famille figurant dans les documents : ☐ même que ci-dessous ou : _____

☐ M. ☐ Mme ☐ Mlle Nom de famille : _____

Prénom : _____ Second prénom : _____

Adresse : (Rue/numéro d'appartement/C.P./R.R.) : _____

_____

Cité ou ville : _____ Province : _____

Code postal : _____

Numéro de téléphone (jour) : _____ Numéro de téléphone (soir) : _____

Description détaillée des documents ou des renseignements personnels demandés ou des renseignements personnels à rectifier. (Si vous présentez une demande d'accès à des renseignements personnels vous concernant ou de rectification de ceux-ci, veuillez indiquer la banque de renseignements personnels ou le document contenant ces renseignements, si vous le savez.)

_____

_____

_____

_____

_____

Remarque : Si vous présentez une demande de rectification de renseignements personnels, veuillez indiquer la rectification demandée et, s'il y a lieu, annexer les documents à l'appui. Si la rectification n'est pas effectuée, vous en serez avisé ou avisée et vous pourrez exiger qu'une déclaration de désaccord soit annexée aux renseignements personnels vous concernant.

Mode préféré d'accès aux documents : ☐ Consulter l'original ☐ Recevoir une copie

_____ Signature _____ Date

À l'usage exclusif du Conseil		
Date de réception :	Numéro de la demande :	Remarque :

Les renseignements personnels figurant sur ce formulaire sont recueillis conformément à la *Loi sur l'accès à l'information municipale et la protection de la vie privée* et seront utilisés pour donner suite à votre demande. Si vous avez des questions sur cette collecte, veuillez les adresser au coordonnateur ou à la coordonnatrice de l'accès à l'information et de la protection de la vie privée au 416 614-5893.