DIRECTIVE RELATIVE AUX RÈGLES ENCADRANT LA GOUVERNANCE DU CENTRE DE SERVICES SCOLAIRE DE MONTRÉAL À L'ÉGARD DES RENSEIGNEMENTS PERSONNELS

Responsabilité
Bureau des affaires juridiques

Adoption
Formulaire de délégation de pouvoirs A-34-3360 adopté par la directrice générale en date du 28 mai 2024

Entrée en vigueur le
29 mai 2024

Centre de services scolaire de Montréal

Québec

Table des matières

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

Préambule et encadrement légal

La présente *Directive relative aux règles encadrant la gouvernance du Centre de services scolaire de Montréal à l'égard des renseignements personnels* (ci-après la « **Directive** ») découle des articles 52.2 et 63.3 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1 (ci-après la « **LAI** *»).*

Dans le cadre de l'exercice de ses fonctions, le Centre de services scolaire de Montréal (ci-après le « **CSSDM** ») assure le traitement de nombreux renseignements personnels. À cet égard, le CSSDM reconnait qu'il est responsable des renseignements personnels qu'il détient aux fins de l'accomplissement de sa mission et il entend prendre les mesures requises pour respecter la vie privée des personnes concernées.

Objectifs

1. La présente Directive a pour objectif de doter le CSSDM de règles encadrant sa gouvernance à l'égard des Renseignements personnels qu'il détient dans le cadre de ses fonctions.
2. Elle vise également à informer toute personne susceptible de transmettre des Renseignements personnels au CSSDM des règles applicables à leur collecte, utilisation, communication, conservation et destruction.
3. Plus précisément, les objectifs de la présente Directive se détaillent comme suit :
   - 3.1. Déterminer les rôles et responsabilités des personnes visées par la présente Directive ;
   - 3.2. Énoncer les obligations et les principes sur lesquels repose la protection des Renseignements personnels collectés, utilisés, communiqués et conservés dans le cadre des fonctions du CSSDM ;
   - 3.3. Déterminer les mesures de protection à appliquer à l'égard des Renseignements personnels collectés ou utilisés dans le cadre d'un Sondage ;
   - 3.4. Établir un processus de traitement des plaintes relatives à la protection des Renseignements personnels ;
   - 3.5. Décrire les activités de formation et de sensibilisation portant sur la protection des Renseignements personnels offertes aux membres du personnel ;
   - 3.6. Établir un processus de gestion des Incidents de confidentialité impliquant des Renseignements personnels ;
   - 3.7. Déterminer des règles encadrant la réalisation d'une Évaluation des facteurs relatifs à la vie privée ;
   - 3.8. Établir les conditions et les modalités suivant lesquelles le CSSDM peut communiquer un Renseignement personnel, sans le consentement de la Personne concernée, en vue de prévenir un acte de violence, dont un suicide.

Champ d'application

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

4. La présente Directive s'applique aux Employés ainsi qu'aux membres du Conseil d'administration, des conseils d'établissement et des différents comités du CSSDM.

Définitions

5. Dans la présente Directive, on entend par :

   5.1. **Acte de violence** : Un acte appréhendé qui engendre un risque sérieux de mort ou de blessures graves ;

   5.2. **Comité sur l'accès** : Comité sur l'accès à l'information et la protection des Renseignements personnels du CSSDM, sur lequel siègent notamment les Responsables de la protection des Renseignements personnels et de l'accès aux documents ;

   5.3. **Commission** : Commission d'accès à l'information du Québec ;

   5.4. **Consentement :** Accord, acquiescement, assentiment volontaire de la Personne concernée à la collecte, l'utilisation ou la communication de Renseignements personnels. Pour être valide, sous réserve d'autres exigences prévues à la LAI, ce consentement doit être manifeste, libre, éclairé et donné à des fins spécifiques. Il doit être demandé en des termes clairs et il ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il est demandé ;

   5.5. **Critère de nécessité** : Applicable notamment dans le cadre de la collecte d'un Renseignement personnel ou dans le contexte où un Employé souhaite avoir accès à un tel renseignement dans l'exercice de ses fonctions, le Critère de nécessité va au-delà de la simple utilité. De façon générale, le Critère de nécessité est démontré si la collecte ou l'utilisation d'un Renseignement personnel répond à toutes ces conditions :

      5.5.1. Son objectif est légitime, important et réel ;

      5.5.2. L'atteinte à la vie privée de la personne est proportionnelle à l'objectif poursuivi ;

      5.5.3. L'atteinte au droit à la vie privée est minimisée, de sorte qu'il n'existe pas d'autres moyens d'atteindre les mêmes objectifs d'une façon qui porte moins atteinte à la vie privée ;

      5.5.4. La collecte, l'utilisation ou la communication du Renseignement personnel est nettement plus utile au CSSDM que préjudiciable à la Personne concernée.

   5.6. **Droits d'accès et de rectification** : Conformément à la LAI et sauf exception, toute Personne concernée par des Renseignements personnels détenus par le CSSDM dispose notamment des droits suivants lorsqu'elle en fait la demande :

      5.6.1. Le droit de recevoir communication d'un tel renseignement en lui permettant d'en prendre connaissance sur place pendant les heures habituelles de travail ou à distance et d'en obtenir une copie ;

      5.6.2. Le droit de demander la rectification d'un fichier qui contient un Renseignement personnel qui la concerne si celui-ci est inexact, incomplet ou équivoque ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la LAI ;

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

5.7. **Employés :** Personnes membres du personnel du CSSDM, incluant les stagiaires et les bénévoles ;

5.8. **Évaluation des facteurs relatifs à la vie privée (« ÉFVP ») :** Démarche préventive d'évaluation qui consiste à considérer tous les facteurs d'un projet qui entraînerait des conséquences positives ou négatives sur le respect de la vie privée des Personnes concernées afin d'identifier des mesures propres à mieux protéger leurs Renseignements personnels et à respecter davantage leur vie privée ;

5.9. **Incident de confidentialité** : Il peut d'agir, selon le cas :

5.9.1. D'un accès non autorisé par la Loi à un Renseignement personnel ;

5.9.2. D'une utilisation non autorisée par la Loi d'un Renseignement personnel ;

5.9.3. De la communication non autorisée par la Loi d'un Renseignement personnel ;

5.9.4. De la perte d'un Renseignement personnel ;

5.9.5. De toute autre atteinte à la protection d'un tel renseignement.

5.10. **Personne concernée :** Personne physique concernée par le Renseignement personnel collecté, utilisé ou communiqué qui est apte à consentir ou lorsqu'applicable, son représentant légal ou le titulaire de l'autorité parentale. Sans limiter la généralité de ce qui précède et sauf exception, le titulaire de l'autorité parentale consent pour un mineur de moins de 14 ans. Le mineur de 14 ans et plus ou le titulaire de l'autorité parentale consent pour le mineur de 14 ans et plus ;

5.11. **Renseignement personnel :** Renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier. Le terme « Renseignement personnel » inclut en tout temps les Renseignements personnels anonymisés, dépersonnalisés et sensibles. Les Renseignements personnels peuvent être classés par regroupements, dont voici des exemples :

- Renseignements d'identification : nom, numéro de fiche, code permanent, adresse, numéro de permis de conduire, date de naissance, numéro d'assurance sociale, numéro d'assurance maladie, numéro de passeport, etc.
- Renseignements de nature financière : numéro de carte de crédit, numéro de carte de débit, renseignement bancaire (hypothèque, numéro de compte, placement, numéro d'identification personnel [NIP]) contrat de travail, salaire, etc.
- Renseignements scolaires/académiques : les résultats, niveaux de difficultés, plan d'intervention, difficulté de comportement, etc.
- Renseignements de nature médicale ou génétique : diagnostic médical, historique médical, arrêt de travail, etc.
- Renseignements démographiques : orientation sexuelle, identité de genre, religion, origine ethnique, niveau de scolarité, état matrimonial, etc.

5.12. **Renseignement personnel anonymisé :** Renseignement personnel dont il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement la Personne concernée ;

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

5.13. **Renseignement personnel dépersonnalisé :** Renseignement personnel qui ne permet plus d'identifier directement la Personne concernée ;

5.14. **Renseignement personnel sensible :** Renseignement personnel qui, par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée ;

5.15. **Requérant :** personne qui transmet au CSSDM une demande d'accès aux documents ou une demande de communication ou de rectification d'un Renseignement personnel en vertu de la LAI ;

5.16. **Responsable :** Responsable de la protection des Renseignements personnels ;

5.17. **Risque de préjudice sérieux :** Un Risque de préjudice sérieux consiste en un évènement qui causerait une perte ou un préjudice important à une personne au niveau du respect de son intimité ou de sa vie personnelle. Dans ce cas-ci, la perte ou le préjudice n'a pas besoin d'être tangible : les effets de l'atteinte à la vie privée peuvent être manifestes et externes (ex. : dommage à la réputation), ou être vécus de l'intérieur par les Personnes concernées (ex. : sentiment d'intrusion) ;

5.18. **Sondage :** Méthode statistique de collecte de données visant à interroger une partie d'une population en utilisant des concepts, des méthodes ou des procédures généralement reconnus dans le domaine des statistiques. Aux fins de la présente Directive, les Sondages incluent aussi les questionnaires ou formulaires transmis à un ensemble de personnes ainsi que les entrevues individuelles ou en groupe ;

5.19. **Traitement des Renseignements personnels** : désigne l'ensemble des étapes du cycle de vie d'un Renseignement personnel ou chacune d'entre elles distinctement. Les étapes du cycle de vie d'un Renseignement personnel sont : la collecte, l'utilisation, la conservation, la communication et la destruction ;

5.20. **Unité administrative :** Réfère, selon le cas, aux services et bureaux administratifs ainsi qu'aux établissements scolaires du CSSDM.

Collecte, utilisation, communication, conservation et destruction des Renseignements personnels

6. À chaque étape du cycle de vie des Renseignements personnels, des mesures propres à assurer leur protection doivent être mises en place. Ainsi, le Traitement de tels Renseignements doit être réalisé dans le respect des exigences et principes décrits ci-dessous.

7. **Collecte**

7.1. Avant de collecter un Renseignement personnel, un Employé doit déterminer les fins (ou les objectifs) de la collecte, lesquelles doivent être Nécessaires à l'exercice des fonctions du CSSDM (ex. : ouvrir un compte, traiter une demande d'inscription, répondre à une plainte, etc.).

7.2. Un Employé doit collecter uniquement les Renseignements personnels qui sont requis pour atteindre les fins déterminées.

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

7.3. Une collecte effectuée à un autre titre pourra être permise dans les cas prévus à la LAI, si elle est préalablement autorisée par le Responsable.

7.4. Généralement, la collecte de Renseignements personnels est effectuée auprès de la Personne concernée ou son représentant. Lors de cette collecte, les informations suivantes doivent être transmises :

7.4.1. Le nom de l'organisme public au nom de qui la collecte est faite ;

7.4.2. Les fins pour lesquelles ces renseignements sont recueillis ;

7.4.3. Les moyens par lesquels les renseignements sont recueillis ;

7.4.4. Le caractère obligatoire ou facultatif de la demande ;

7.4.5. Les conséquences d'un refus de répondre à la demande ou, le cas échéant, d'un retrait de son Consentement à la communication ou à l'utilisation des renseignements collectés suivant une demande facultative ;

7.4.6. Les Droits d'accès et de rectification prévus à la LAI ;

7.4.7. S'il y a lieu, le nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer ces renseignements ;

7.4.8. S'il y a lieu, informer la Personne concernée de la possibilité que ces renseignements soient communiqués à l'extérieur du Québec ;

7.4.9. Sur demande de la personne, toutes autres informations requises par la LAI et qui sont applicables à la situation en cause.

7.5. Si la collecte est effectuée auprès de la Personne concernée en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci, la Personne concernée doit au préalable être informée :

7.5.1. Du recours à une telle technologie ;

7.5.2. De moyens offerts pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage.

7.6. Toute collecte de Renseignements personnels concernant un mineur de moins de 14 ans ne peut être effectuée auprès de celui-ci sans le Consentement du titulaire de l'autorité parentale ou du tuteur, sauf lorsque cette collecte est manifestement au bénéfice de ce mineur. Dans ce cas, le Responsable doit en être préalablement informé.

7.7. Toute collecte d'un Renseignement personnel visant à offrir un produit ou un service technologique disposant de paramètres de confidentialité doit être effectuée de manière à ce que par défaut, ces paramètres assurent le plus haut niveau de confidentialité, sans aucune intervention de la Personne concernée. Les paramètres de confidentialité d'un témoin de connexion ne sont toutefois pas visés.

8. **Utilisation**

8.1. Un Employé peut utiliser un Renseignement personnel pour les fins pour lesquelles il a été collecté.

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

8.2. Une utilisation à une autre fin sera permise avec le Consentement de la Personne concernée.

8.3. Dans la mesure du possible, un tel Consentement doit être obtenu de manière expresse, c'est-à-dire être explicitement exprimé par un geste ou une déclaration témoignant de l'acceptation par la Personne concernée, préférablement par écrit. Un Consentement exprès ne laisse aucun doute sur la volonté réelle de la personne.

8.4. Lorsqu'il s'agit d'un Renseignement personnel sensible, le Consentement doit être obtenu de manière expresse.

8.5. Une utilisation à une autre fin peut être permise sans le Consentement de la Personne concernée uniquement dans les situations prévues à la Loi.

8.6. Le Responsable doit être consulté pour toute autre utilisation fondée sur une exception prévue à la Loi. Le cas échéant, une consignation est faite au registre prévu à cet égard.

9. Accès aux Renseignements personnels dans l'exercice des fonctions

9.1. Un Employé a accès, sans le Consentement de la Personne concernée, à un Renseignement personnel lorsqu'il a la qualité pour le recevoir (à la lumière de sa description de tâches et de ses responsabilités, de façon explicite ou non) et que ce renseignement est nécessaire à l'exercice de ses fonctions.

9.2. Les accès aux Renseignements personnels consignés dans des fichiers ou des bases de données doivent faire l'objet d'une révision périodique.

10. Communication

10.1. Un Employé ne peut pas transmettre un Renseignement personnel à une personne qui ne détient pas les autorisations requises pour le recevoir sans le Consentement de la Personne concernée.

10.2. Dans la mesure du possible, le Consentement obtenu devrait être de manière expresse, c'est-à-dire être explicitement exprimé par un geste ou une déclaration témoignant de l'acceptation par la Personne concernée, préférablement par écrit. Un Consentement exprès ne laisse aucun doute sur la volonté réelle de la personne.

10.3. Lorsqu'il s'agit d'un Renseignement personnel sensible, le Consentement doit être obtenu de manière expresse.

10.4. Communication de Renseignements personnels dans le cadre de l'exécution d'un contrat de service ou d'entreprise

10.4.1. Conformément à l'article 67.2 LAI, un Employé peut communiquer un Renseignement personnel dans le Consentement de la Personne concernée à toute personne ou à tout organisme, si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de services ou d'entreprise. Pour ce faire, l'Employé doit :

- S'assurer de la nécessité de communiquer un tel Renseignement personnel dans le cadre du contrat ;
- Inclure des exigences concernant la protection des Renseignements personnels dans les documents d'appel d'offres ou dans le contrat écrit (ex :

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

obligation d'héberger les Renseignements personnels au Québec, l'obligation de détruire les Renseignements une fois les fins pour lesquelles ils ont été collectés ou transmis sont accomplies, transmission des politiques de confidentialité du fournisseur, etc.) ;

- Obtenir des engagements de confidentialité des Employés du fournisseur qui pourraient avoir accès à des Renseignements personnels ;
- Acquérir des avis concernant toute violation ou tentative de violation d'une obligation relative à la confidentialité ;
- Etc.

10.5. **Communication de Renseignements personnels exigés par les services de police ou requis par assignation, citation à comparaître, mandat ou ordonnance d'une personne ayant le pouvoir de contraindre à leur communication**

10.5.1. Un Employé peut communiquer des Renseignements personnels sans le Consentement de la Personne concernée dans les cas prévus par la Loi ou lorsqu'il y est contraint par assignation, citation à comparaître, mandat ou ordonnance. Pour ce faire, un Employé doit :

- Vérifier que l'organisme agit en vertu d'un pouvoir prévu à la loi permettant de contraindre à la communication de tels renseignements. Le cas échéant, le Bureau des affaires juridiques peut être consulté au préalable ;
- Il doit obtenir une demande écrite et consigner l'ensemble de la documentation transmise ;
- Utiliser le formulaire approprié pour les demandes provenant des services de police dans le cadre d'une enquête ou provenant de la Direction de la protection de la jeunesse dans le cadre d'une intervention (formulaires J020 et J021).

10.6. **Conditions et modalités suivant lesquelles le CSSDM peut communiquer un Renseignement personnel en vue de prévenir un Acte de violence, dont un suicide**

10.6.1. Conformément aux articles 59, 59.1, 60 et 60.1 LAI, un Employé peut communiquer un Renseignement personnel sans le Consentement de la Personne concernée lorsqu'il existe un motif raisonnable de croire qu'un Acte de violence menace une personne ou un groupe de personnes identifiables et que la nature de la menace inspire un sentiment d'urgence.

10.6.2. **Conditions**

10.6.2.1. Pour justifier la communication d'un Renseignement personnel sans le Consentement de la Personne concernée, les conditions suivantes doivent être réunies :

- L'existence d'un motif raisonnable de croire qu'il existe un danger menaçant une personne ou un groupe de personnes. Le danger n'a pas à être certain, mais il faut que des circonstances ou des faits concrets

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

permettent à une personne raisonnable, placée dans la même situation, de conclure à un danger d'Acte de violence.

- La personne ou le groupe de personnes menacées doit être identifiable ;
- Le danger auquel la personne ou le groupe de personnes est exposé doit être imminent et immédiat.

10.6.3. **Contenu de la communication**

10.6.3.1. Seuls les Renseignements personnels nécessaires aux fins poursuivies par la communication, en l'occurrence la prévention d'un Acte de violence, peuvent être communiqués.

10.6.3.2. Ces Renseignements personnels peuvent être, notamment : l'identité et les coordonnées de la personne en danger et de celle qui a proféré les menaces, ainsi que la nature de la menace et les circonstances dans lesquelles elles ont été proférées.

10.6.4. **Formalités à respecter**

10.6.4.1. Lorsque toutes les conditions ci-haut décrites sont réunies, l'Employé peut alors communiquer les Renseignements personnels à la ou aux personnes exposées à ce danger, à leur représentant ou à toute personne susceptible de leur porter secours.

10.6.4.2. Le représentant de ces personnes peut être un parent ou, s'il s'agit d'un groupe de personnes, celle qui agit à titre de Responsable.

10.6.4.3. Les personnes susceptibles de leur porter secours peuvent être, notamment : un policier, un centre de prévention du suicide, un organisme d'aide et de soutien aux victimes d'actes de violence, un CLSC, un professionnel de la santé ou un directeur de la protection de la jeunesse.

10.6.4.4. À défaut de s'être assuré que les Renseignements personnels visés sont nécessaires pour les fins décrites au présent article, l'Employé ne doit pas communiquer le Renseignement personnel.

10.6.4.5. L'Employé doit, dans la mesure où les circonstances le permettent, obtenir l'autorisation de son supérieur immédiat avant de communiquer un Renseignement personnel.

10.6.4.6. Advenant qu'aucune autorisation ne puisse être obtenue promptement et qu'une décision doive être prise considérant l'urgence de la situation, l'Employé doit agir selon ce qu'il juge le plus approprié compte tenu des circonstances.

10.6.4.7. Suite à la communication de tout Renseignement personnel en vertu du présent article, l'Employé qui effectue la communication doit remplir et transmettre au Responsable, dans les meilleurs délais, le formulaire joint en Annexe I pour que ladite communication soit consignée au registre tenu à cette fin.

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

10.7. Le Responsable peut être consulté pour toute communication d'un Renseignement personnel sans le Consentement de la Personne concernée dans les cas prévus à la loi.

11. **Conservation et destruction**

11.2. Un Employé doit connaitre et appliquer les mesures de sécurité déterminées par le CSSDM pour chaque Renseignement personnel auquel il a accès.

11.3. À défaut, un Employé doit prendre les mesures de sécurité propres à assurer la protection des Renseignements personnels auxquelles il a accès, et qui sont raisonnables compte tenu notamment de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

11.4. Lorsqu'un Employé est informé ou a des motifs raisonnables de croire que les Renseignements personnels qu'il conserve ne sont plus à jour, exacts ou complets pour servir aux fins pour lesquelles ils sont collectés ou utilisés, il en avise rapidement la direction de son Unité administrative afin que les mesures appropriées soient prises.

11.5. Un Employé doit connaitre et appliquer le calendrier de conservation et le plan de classification du CSSDM relevant du Secteur de la gestion documentaire et des archives.

11.6. À défaut, un Employé doit prendre les mesures pour détruire de manière sécuritaire un Renseignement personnel qu'il conserve lorsque les fins pour lesquelles il a été collecté ou utilisé sont accomplies. De telles mesures doivent être raisonnables en fonction notamment de la sensibilité, de la quantité et du support du Renseignement personnel en cause.

Gestion des Consentements

12. Lorsque requis, le Consentement de la Personne concernée doit comporter les caractéristiques suivantes :

    1. Manifeste : évident et donné d'une façon qui démontre la volonté réelle de la personne.
    2. Libre : impliquant un choix réel et donné sans contrainte ni pression indue
    3. Éclairé : précis, donné en connaissance de cause et avec toutes les informations nécessaires en des termes simples et clairs pour comprendre la portée du Consentement
    4. Spécifique : donné dans un objectif précis et clairement circonscrit pour chaque fin et valide seulement pour la durée nécessaire

13. Le Consentement concernant un Renseignement personnel sensible doit être manifesté de façon expresse, c'est-à-dire explicitement exprimé par un geste ou une déclaration (orale ou écrite) témoignant de l'acceptation par la Personne concernée. Un Consentement exprès ne laisse aucun doute sur la volonté réelle d'une personne (exemples : signature d'un formulaire, activation d'une case, réponse affirmative à une question, approbation verbale).

14. Un Employé doit offrir l'assistance requise à la Personne concernée pour l'aider à comprendre la portée du Consentement. Dans ce cas, les coordonnées de l'Unité administrative visée devraient être données à la Personne concernée, préférablement par écrit, notamment dans l'éventualité où la Personne souhaite retirer son Consentement.

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

15. Dans l'éventualité où la Personne concernée souhaite retirer son Consentement à la communication ou à l'utilisation des Renseignements personnels, l'Unité administrative doit informer cette personne des conséquences du retrait de son Consentement.

16. L'Unité administrative concernée doit s'assurer qu'elle obtient le Consentement de la Personne concernée ou veiller à vérifier la qualité du représentant légal d'un mineur de moins de 14 ans (titulaire de l'autorité parentale, représentant ou mandataire). Lorsque nécessaire, la vérification de l'identité peut se faire par plusieurs moyens, notamment : la vérification d'une pièce d'identité avec photo en personne ou en vidéoconférence, l'utilisation de secrets partagés, etc.

17. Le cas échéant, la preuve écrite du Consentement doit être conservée au moins tout au long de l'utilisation des Renseignements personnels en cause et par la suite, en fonction du calendrier de conservation du CSSDM. Lorsque le Consentement est requis verbalement, l'Employé doit consigner les circonstances dans lesquelles le Consentement a été donné (ex. : date du Consentement, identité de la Personne concernée ou de son représentant légal, etc.).

Projets particuliers nécessitant la réalisation d'une Évaluation des facteurs relatifs à la vie privée

18. Un Employé d'un service ou d'un bureau administratif qui est responsable d'un projet visé aux articles 63.5, 64, 65.5, 67.3.1, 68 et 70.1 de la LAI doit s'assurer qu'une Évaluation des facteurs relatifs à la vie privée est effectuée sous la coordination du Responsable et que toutes les conditions prévues dans la LAI soient respectées.

19. Un Employé d'un service ou d'un bureau administratif qui est responsable d'un projet visé aux articles 64, 67.2, 67.2.1, 68 et 70.1 de la LAI doit s'assurer qu'une entente ou un contrat écrit a été conclu sous la direction du Responsable et est en vigueur avant de procéder à toute collecte, utilisation ou communication de Renseignements personnels.

20. La réalisation d'une Évaluation des facteurs relatifs à la vie privée est encadrée par la procédure présentée en Annexe II.

Processus de gestion des Incidents de confidentialité impliquant des Renseignements personnels

21. **Procédure de déclaration des Incidents de confidentialité**

    21.1. L'Employé qui a des motifs de croire qu'un Incident de confidentialité est survenu doit, sans délai, le déclarer au Responsable.

    21.2. La déclaration doit être faite à l'adresse courriel suivante : accesdoc@cssdm.gouv.qc.ca.

    21.3. Dans la mesure du possible, le Déclarant consigne les informations suivantes relativement à l'Incident de confidentialité qu'il croit être survenu :

- Le contexte et les circonstances entourant l'événement (dates, description des faits, etc.) ;
- La nature des Renseignements personnels en cause (par exemple : noms, adresse, courriel, code permanent, etc.) ;
- Les mesures de protection qui étaient en place au moment des faits ;

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

- Le nombre de Personnes concernées par l'Incident de confidentialité et leurs coordonnées ;
- L'identité et le nombre de personnes qui ont reçu les Renseignements personnels sans autorisation le cas échéant ;
- Les mesures immédiates prises le cas échéant ;
- Toute autre information pertinente.

21.4. Dans les meilleurs délais, le Déclarant doit informer la direction de son Unité administrative de l'Incident.

21.5. Le Responsable analyse sommairement la situation déclarée et détermine s'il s'agit d'un Incident de confidentialité impliquant des Renseignements personnels.

21.6. S'il détermine qu'il ne s'agit pas d'un Incident de confidentialité, mais qu'il juge qu'une intervention est tout de même nécessaire auprès des personnes impliquées dans l'événement, il communique avec la direction de l'Unité administrative visée afin qu'elle pose, le cas échéant, les actions requises.

22. **Mise en application de mesures d'atténuation immédiates**

22.1. Lorsque les circonstances le permettent, le Responsable met en application des mesures d'atténuation immédiates pour éviter qu'un préjudice ne soit causé aux Personnes concernées ou qu'un Incident de confidentialité de même nature ne survienne. Pour ce faire, le Responsable peut faire appel à tout Employé dont l'aide ou l'expertise est requise, dont notamment le Chef de la sécurité de l'information organisationnelle.

22.1.1. Les mesures d'atténuation immédiates peuvent comprendre :

22.1.2. La fermeture de tout serveur ou logiciel informatique ;

22.1.3. Rappeler des courriels ;

22.1.4. Révoquer ou modifier des mots de passe ou des codes d'accès ;

22.1.5. Etc.

22.2. Le cas échéant, le Responsable, en collaboration avec la direction de l'Unité administrative concernée, veille à obtenir des personnes à qui ont été illégalement communiqués des Renseignements personnels, une confirmation de destruction ou un engagement de non-divulgation de ces renseignements.

22.3. Selon le cas, le Responsable veille à informer les principaux intervenants concernés par l'Incident de confidentialité : direction générale, direction du Service des communications et affaires publiques, service de police (si les circonstances portent à croire qu'un crime a été commis), assureurs, ministère de l'Éducation (en cas de cyberattaque, par exemple), etc.

23. **Évaluation du Risque de préjudice sérieux**

23.1. Le Responsable coordonne l'évaluation du Risque de préjudice sérieux de l'Incident de confidentialité en considérant notamment la sensibilité du Renseignement, les

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. Cette évaluation doit se faire à l'aide de la grille d'évaluation jointe en Annexe III.

24. **Mesures à prendre lorsque l'Incident de confidentialité présente un Risque de préjudice sérieux**

24.1. Si l'Incident de confidentialité présente un Risque de préjudice sérieux, le Responsable doit veiller à ce que :

24.1.1. La Commission d'accès à l'information du Québec soit avisée de l'Incident de confidentialité avec diligence, de la manière et en fournissant les informations requises ;

24.1.2. Toute personne dont les Renseignements personnels sont en cause par l'Incident de confidentialité soit informée et en fournissant les informations requises ;

24.1.3. Tout organisme susceptible de diminuer le Risque de préjudice sérieux soit informé (ministère, police, spécialiste en gestion de crise, etc.) en ne communiquant que les Renseignements personnels nécessaires à cette fin.

24.2. Aucun avis aux personnes visées n'est nécessaire si un tel avis avait pour effet d'entraver une enquête faite par une personne ou par un organisme qui, en en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

25. **Registre des Incidents de confidentialité**

25.1. Le Responsable inscrit l'Incident de confidentialité impliquant des Renseignements personnels au registre des Incidents de confidentialité dans tous les cas.

26. **Mesures à prendre pour éviter qu'un Incident de confidentialité de même nature se reproduise**

26.1. Une fois les mesures immédiates mises en place, le Responsable détermine si d'autres mesures doivent être appliquées pour éviter que des Incidents de confidentialité de même nature ne se reproduisent. Ces mesures peuvent comprendre : la modification des accès informatiques, des rappels des bonnes pratiques, la révision de processus internes, etc.

26.2. Afin de mettre en place les mesures correctrices identifiées, le Responsable peut faire appel à toute personne dont l'aide lui est nécessaire, dont notamment la direction d'une Unité administrative.

Mesures de protection particulières lors d'un Sondage

27. **Sondage visé**

27.1. Seul un Sondage visant la collecte ou l'utilisation de Renseignements personnels est visé par la présente Directive, que celui-ci soit réalisé auprès des élèves et leurs parents ou après des Employés.

27.2. Le cas échéant, tous les types de Sondages sont visés, qu'importe le format et le support (ex. : sondages d'opinion ou d'intention, de satisfaction, de mesure de la qualité des

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

services, études de marché, sondages sous forme d'entrevue individuelle ou de groupe, sondages automatisés de type FORMS).

27.3. Sont aussi assujettis à la présente Directive, avec les adaptations nécessaires, les Sondages menés par des tiers pour le compte du CSSDM ou ceux élaborés par des partenaires, tels que les chercheurs externes dont les projets de recherche sont aussi encadrés par le Protocole applicable dans le cadre des demandes d'expérimentation dans le cadre de recherches scientifiques. Par conséquent, lors de la conclusion d'une telle entente avec un tiers ou un partenaire, le CSSDM est responsable d'assurer le respect de la présente section de la Directive.

28. **Nécessité**

28.1. Un Employé doit, avant de réaliser un Sondage, évaluer la nécessité de recourir au Sondage dans la cadre de la mission du CSSDM. Plus précisément, les Sondages menés auprès des élèves, des parents ou après des Employés doivent s'inscrire dans l'atteinte des objectifs du CSSDM, notamment ceux de nature éducative, financière, environnementale, etc.

28.2. Le CSSDM privilégie les Sondages dont la réalisation ne nécessite pas la collecte de Renseignements personnels, à moins que cela ne soit nécessaire à l'atteinte des objectifs du Sondage. Dans tous les cas, le CSSDM s'assure de limiter la quantité de Renseignements personnels utilisés et évite de collecter des Renseignements personnels sensibles.

29. **La planification du Sondage**

29.1. Avant de réaliser un Sondage, l'Employé doit :

29.1.1. Établir les objectifs du Sondage ;

29.1.2. Procéder à une évaluation de l'aspect éthique du Sondage, compte tenu notamment de la nature et de l'objet du Sondage, des personnes visées, de la sensibilité des Renseignements personnels collectés et de la finalité de l'utilisation de ceux-ci, avec au besoin le soutien du conseiller en éthique du CSSDM ;

29.1.3. Identifier les Renseignements personnels collectés et préparer les autorisations nécessaires pour les participants au Sondage ;

29.1.4. Établir un plan de Sondage en identifiant de façon non limitative les éléments suivants, et ce en conformité avec les exigences légales et les principes établis dans la présente Directive :

- les personnes ou les catégories de personnes qui auront accès aux Renseignements personnels utilisés ou collectés dans le cadre du Sondage. Seules peuvent avoir accès aux Renseignements personnels collectés les personnes qui le nécessitent dans le cadre de leurs fonctions ;
- le lieu de conservation ou de stockage des données en conformité avec les normes de stockage de l'information numérique. Dans le cas des sondages automatisés de type FORMS, une fois que les données ont été transférées

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

dans leur lieu de conservation, le Sondage doit être supprimé de son environnement de production ;

- les mesures de sécurité qui seront applicables pour assurer la protection des Renseignements personnels ;
- la durée de leur conservation et les modalités de leur destruction, conformément au calendrier de conservation ;
- Au besoin, réaliser une Évaluation des facteurs relatifs à la vie privée.

29.2. Avant de réaliser le Sondage, l'Employé ou le tiers doit obtenir l'autorisation de la direction de son Unité administrative.

29.3. Le Responsable ou le Comité sur l'accès peuvent être consultés.

30. **La réalisation du Sondage**

30.1. Conformément à la LAI, l'Employé ou le tiers qui collecte des Renseignements personnels dans le cadre d'un Sondage doit informer la Personne concernée des éléments identifiés à l'article 7.4 de la présente Directive avec les adaptations nécessaires.

30.2. Lorsqu'applicable, l'Employé ou le tiers doit informer le répondant que sa participation est volontaire et qu'aucune conséquence ne découlera de son refus de participer.

30.3. Indiquer dans la communication ou le courriel d'invitation à participer au Sondage, le délai maximal pour y répondre.

31. **Publication des résultats**

31.1. Le cas échéant, la publication des résultats du Sondage (auprès d'autres personnes qui celles qui le nécessitent dans le cadre de leurs fonctions) ne doit pas contenir des renseignements permettant d'identifier directement ou indirectement les participants, et ce, que ces derniers y aient consenti ou non. Une attention particulière doit être portée aux réponses des questions ouvertes et aux combinaisons de réponses afin que celles-ci ne permettent pas d'identifier indirectement le répondant.

31.2. Les Renseignements personnels collectés lors de la réalisation d'un Sondage doivent être détruits de façon sécuritaire suite à leur analyse ou leur interprétation. Le cas échéant, le CSSDM peut aussi anonymiser ces renseignements pour les utiliser à des fins d'intérêt public.

Activités de formation et de sensibilisation

32. Lors de l'entrée en fonction d'un Employé et au besoin par la suite, une copie de la présente Directive lui est remise avec les informations nécessaires à sa compréhension.

33. Lors de son entrée en fonction, un Employé doit signer un engagement au respect à la protection des Renseignements personnels.

34. Régulièrement, la direction d'une Unité administrative, en collaboration avec le Responsable, veille à ce que les Employés sous sa responsabilité soient sensibilisés relativement aux exigences et principes entourant la protection des Renseignements personnels, notamment :

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

34.1. Leurs rôle et responsabilités ;

34.2. Les mesures de sécurité applicables ;

34.3. Les règles entourant la conservation et la destruction des Renseignements personnels ;

34.4. L'identification et la gestion des Incidents de confidentialité impliquant des Renseignements personnels.

35. Les activités de sensibilisation sont effectuées de différentes manières : capsules de formation, séances de discussion, courriel d'information, etc.

36. En fonction des besoins particuliers, le Responsable peut identifier des formations ou des activités de sensibilisation qui doivent être mises en place pour une catégorie d'Employés ou pour une Unité administrative spécifique.

Processus de traitement des plaintes

37. **Dépôt d'une plainte et son contenu**

37.1. Conformément au processus de traitement des plaintes liées aux fonctions du CSSDM, une personne peut formuler une plainte auprès du Responsable relativement au non-respect par le CSSDM de ses obligations en matière de protection des Renseignements personnels.

37.2. Les coordonnées du Responsable sont diffusées sur la page portant sur le traitement des plaintes du site Internet du CSSDM, dans la section appropriée.

37.3. La plainte doit comporter une description des faits à l'origine de la plainte, incluant la période visée, les Renseignements personnels en cause et la nature du redressement demandé.

37.4. Dans le cas où la plainte implique la conduite du Responsable, la plainte doit être transmise aux coordonnées indiquées sur la page portant sur le traitement des plaintes du site Internet du CSSDM, dans la section concernant les plaintes en lien avec les fonctions du CSSDM. Dans un tel cas, la directrice générale assurera le traitement d'une telle plainte conformément à la section suivante.

38. **Traitement de la plainte**

38.1. Le Responsable accuse réception de la plainte dans un délai raisonnable de la réception.

38.2. Le Responsable peut rejeter sommairement toute plainte frivole, vexatoire ou de mauvaise foi. Il doit alors en informer la personne ayant déposé la plainte.

38.3. Le Responsable peut refuser de traiter une plainte si les faits font l'objet d'un recours en justice, à l'inclusion de toute demande devant de la Commission.

39. **Réponse**

39.1. Le Responsable analyse la plainte et transmet sa conclusion par écrit à la personne ayant déposé la plainte dans les quinze (15) jours ouvrables de la réception de celle-ci.

39.2. Si le Responsable juge que le traitement de la plainte dans le délai prévu de quinze (15) jours ouvrables n'est pas possible en raison de la nature de celle-ci, il peut, avant

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

d'expiration de ce délai, le prolonger d'une période qu'il juge raisonnable et en informer la personne.

39.3. Le cas échéant, le Responsable s'assure de la mise en place des correctifs appropriés.

39.4. En cas de désaccord avec la réponse du Responsable, la personne ayant déposé la plainte peut formuler une plainte à la Commission d'accès à l'information du Québec.

Rôles et responsabilités

40. **Directeur général**

40.1. Déléguer par écrit les fonctions de Responsable ;

40.2. Veiller à faciliter l'exercice des fonctions du Responsable et à préserver son autonomie ;

40.3. Aviser par écrit dès que possible la Commission du titre, des coordonnées et de la date d'entrée en fonction de la personne qui exerce la fonction de Responsable ;

40.4. Transmettre avec diligence au Responsable toute demande d'accès aux documents et toute demande de communication ou de rectification de Renseignements personnels qui lui est adressée par écrit ;

40.5. S'assurer de la mise en place et du bon fonctionnement du Comité sur l'accès ;

40.6. Adopter toute directive ou encadrement qui relève de sa compétence et qui est requis pour assurer le respect de la LAI, et voir à leur mise à jour ;

40.7. Traiter les plaintes relatives à la protection des Renseignements personnels qui impliquent le Responsable.

41. **Comité sur l'accès**

41.1. Soutenir le CSSDM dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la LAI ;

41.2. Approuver la présente Directive et toute mise à jour ;

41.3. Être consulté au début de tout projet d'acquisition, de développement et de refonte des systèmes d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de Renseignements personnels ;

41.4. Suggérer, à toute étape d'un projet visé au paragraphe précédent, des mesures de protection des Renseignements personnels applicables à ce projet ;

41.5. Exercer toute autre fonction en lien avec la protection des Renseignements personnels à la demande du Directeur général.

42. **Responsable**

42.1. En collaboration avec la Responsable de l'accès aux documents :

42.1.1. Recevoir les demandes d'accès aux documents, les demandes de communication ou de rectification de Renseignements personnels, s'assurer qu'elles soient traitées selon les dispositions de la LAI, incluant la transmission de tout avis requis par la LAI et rendre une décision dans le délai prévu ;

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

42.1.2. Prêter assistance au Requérant qui le demande pour l'aider à comprendre la décision transmise ;

42.1.3. Veiller à ce que tout document qui a fait l'objet d'une demande d'accès, de communication ou de rectification de Renseignements personnels soit conservé le temps requis pour permettre au Requérant d'épuiser les recours prévus à la LAI ;

42.2. Coordonner et participer selon les besoins à l'Évaluation des facteurs relatifs à la vie privée pour les projets qui le requièrent ;

42.3. Veiller à l'analyse et prendre position sur l'application d'une situation d'exception prévue à la LAI en matière de collecte, d'utilisation, de communication ou de conservation des Renseignements personnels ;

42.4. Lorsque prévu à la LAI, veiller à la rédaction de mandat, d'entente ou de contrat à intervenir entre le CSSDM et une personne ou un organisme impliquant un Renseignement personnel dont il a la responsabilité ;

42.5. Exercer les responsabilités qui lui sont dévolues lorsque survient un Incident de confidentialité impliquant des Renseignements personnels ;

42.6. S'assurer de la mise en place, de la tenue et de l'inscription des données requises aux différents registres prévus à la LAI ;

42.7. Participer à l'établissement et la mise à jour du plan de classification des documents et du calendrier de conservation ;

42.8. Traiter les plaintes relatives à la protection des Renseignements personnels en conformité avec la présente Directive ;

42.9. Veiller à la sensibilisation et à la formation des Employés en matière de protection des Renseignements personnels en conformité avec la présente Directive ;

42.10. Assurer un rôle de soutien et de conseil relativement à toute question touchant l'accès aux documents ou à la protection des Renseignements personnels ;

42.11. Agir à titre de représentant auprès des autres organismes publics et de la Commission pour toute question relative à l'accès aux documents et à la protection des Renseignements personnels ;

42.12. Exercer toute autre fonction prévue à la LAI ou à la demande du Directeur général.

43. **Direction d'une Unité administrative**

43.1. Veiller au respect de la présente Directive par les Employés sous sa responsabilité ;

43.2. Connaitre, pour son Unité administrative, les Renseignements personnels qu'elle détient et participer à la mise à jour de l'inventaire de ces renseignements ;

43.3. Identifier les Employés sous sa responsabilité qui ont accès à des Renseignements personnels, ainsi que les regroupements de Renseignements personnels qui leur sont accessibles ;

43.4. Mettre en place au sein de son Unité administrative des mesures de protection des Renseignements personnels qui sont élaborées par le Service des technologies de

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

l'information qui sont raisonnables compte tenu notamment de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support et voir à la diffusion et à l'application de ces mesures par les Employés sous sa responsabilité ;

43.5. Appliquer au sein de son Unité administrative une procédure de destruction sécuritaire d'un Renseignement personnel selon les normes élaborées par le Service des technologies de l'information ou le Secteur de la gestion documentaire et des archives ;

43.6. Exercer les responsabilités qui lui sont dévolues relativement aux Incidents de confidentialité impliquant des Renseignements personnels ;

43.7. En collaboration avec le Responsable, veiller à ce que les formations et les activités de sensibilisation prévues à la présente Directive soient offertes aux Employés sous sa responsabilité et s'assurer que ces derniers y participent ;

43.8. Communiquer au besoin avec le Responsable pour toute question relative aux demandes d'accès ou à la protection des Renseignements personnels dans son Unité administrative.

44. **Employé**

44.1. Prendre connaissance et respecter la présente Directive ;

44.2. Participer aux formations et aux activités de sensibilisation prévues à la présente Directive ;

44.3. Utiliser les outils, les documents modèles, les documents de référence ou tout autre document mis à sa disposition pour favoriser le respect de la présente Directive ;

44.4. Collaborer sur demande avec le Responsable lors du traitement d'une demande d'accès à des documents, de communication ou de rectification d'un Renseignement personnel ou de toute autre démarche de même nature au regard de la LAI ;

44.5. Collaborer sur demande avec le Responsable lors du traitement d'une plainte visée par la présente Directive ;

44.6. Communiquer au besoin avec son supérieur immédiat relativement à la présente Directive pour obtenir des précisions, des conseils ou l'informer d'une problématique dans l'application de la présente Directive ou d'un cas particulier.

Entrée en vigueur

45. La présente Directive est approuvée par le Comité sur l'accès.

46. Elle entre en vigueur le jour de son adoption par le directeur général.

Annexes

Les annexes font partie intégrante de la présente Directive.

Annexe I : Formulaire – Communication de Renseignements personnels en vue de prévenir un Acte de violence dont un suicide

Annexe II : À VENIR - Procédure relative à la réalisation d'une Évaluation relative à la vie privée

Annexe III : Grille d'évaluation du Risque de préjudice sérieux (Incident de confidentialité)

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

Annexe IV : Aide-mémoire – *Directive relative aux règles encadrant la gouvernance du CSSDM à l'égard des Renseignements personnels*

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

Pour joindre le service responsable :
accesdoc@cssdm.gouv.qc.ca

cssdm.gouv.qc.ca

Centre de services scolaire de Montréal
Québec

© Centre de services scolaire de Montréal, 2023 / Tous droits réservés.

Centre
de services scolaire
de Montréal
Québec

Communication de renseignements personnels en vue de prévenir un acte de violence, dont un suicide
(Article 59.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels)*

DIRECTION GÉNÉRALE
BUREAU DES AFFAIRES JURIDIQUES

TOUT EFFACER

Conformément aux modalités prévues à la *Directive relative aux règles encadrant la gouvernance du CSSDM à l'égard des renseignements personnels*, un Employé peut communiquer un renseignement personnel sans le consentement de la Personne concernée lorsqu'il existe un motif raisonnable de croire qu'un Acte de violence menace une personne ou un groupe de personnes identifiables et que la nature de la menace inspire un sentiment d'urgence.

Suite à la communication, l'Employé concerné doit remplir et transmettre au Responsable de la protection des renseignements personnels le présent formulaire, dans les meilleurs délais.

Date ou l'employé a pris connaissance du danger menaçant une personne ou un groupe de personnes identifiables	
Date de la communication des renseignements	
Nom de la personne qui a communiqué les renseignements	
Nom de la personne consultée *(le cas échéant)*	

Description du danger et des circonstances de l'événement

Nature des renseignements personnels communiqués

Nom, titre et coordonnées des personnes à qui les renseignements ont été communiqués	

Date de transmission du présent formulaire au Responsable de la protection des renseignements personnels. accesdoc@cssdm.gouv.qc.ca	

GRILLE D'ÉVALUATION DU PRÉJUDICE LORS D'UN INCIDENT DE CONFIDENTIALITÉ

À quoi sert cette grille d'évaluation ?

La grille d'évaluation a pour objectif de permettre au CSSDM de déterminer s'il existe un risque qu'un préjudice sérieux soit causé à une personne dans le cadre d'un incident de confidentialité impliquant un renseignement personnel. Le CSSDM a l'obligation de se soumettre à une telle évaluation afin d'assurer le respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

Est-ce un incident de confidentialité?

1. Nature de l'incident de confidentialité[1] *(dans le cas où aucune de ces situations ne s'applique, il ne s'agit pas d'un incident de confidentialité)*

- ☐ L'accès non autorisé par la loi à des renseignements personnels;
- ☐ L'utilisation non autorisée par la loi des renseignements personnels;
- ☐ La communication non autorisée par la loi de renseignements personnels;
- ☐ La perte de renseignements personnels;
- ☐ Toute autre atteinte à la protection de tels renseignements;

Date ou période de l'évènement	Date de découverte de l'évènement

2. Brève description de l'évènement (circonstances) : *personnes impliquées, comment, s'agit-il d'une erreur, problème de logiciel, vulnérabilité, procédure, quels sont les renseignements personnels visés par l'incident. Vous pourrez utiliser cette même description pour compléter votre registre de confidentialité.*

Nombre de personnes dont les renseignements sont concernés par l'incident de confidentialité	Nombre de personnes ayant eu accès aux renseignements concernés par l'incident de confidentialité (le cas échéant)
(Dans le cas où le nombre n'est pas connu, inscrire une approximation)	

[1] Article 63.9 de la LAI

3. Nature des renseignements personnels :

☐ **Renseignements d'identification :** *nom, numéro de fiche, code permanent, adresse, numéro de permis de conduire*, date de naissance, numéro d'assurance sociale*, numéro d'assurance maladie*, numéro de passeport*…*

☐ **Renseignements de nature financière* :** *numéro de carte de crédit, numéro de carte de débit, renseignements bancaire (hypothèque, numéro de compte, placement, numéro d'identification personnel (NIP)…) contrat de travail, salaire…*

☐ **Renseignements scolaires/académiques :** *résultat, cote…*

☐ **Renseignements de nature médicale* ou génétique* :** *diagnostic médical, plan d'intervention, difficulté de comportement…*

☐ **Renseignements démographiques :** *orientation sexuelle, identité de genre, croyance religieuse, origine ethnique, niveau de scolarité, état matrimonial, opinion politique ou philosophique)*

☐ **Données de géolocalisation* :**

☐ **Autre,** précisez :

Commentaires :

* *Signifie que ces renseignements sont généralement considérés comme étant sensibles.*

N.B. : Il est également possible qu'un renseignement à lui seul ne soit pas considéré comme étant sensible, mais une fois jumelé à d'autres renseignements, il le devient.

4. Quel est le degré de sensibilité des renseignements concernés?

☐ **Les renseignements sont privés, mais étaient déjà rendus publics avant l'incident :** *ex : adresse sur le rôle d'évaluation foncière, la personne a elle-même diffusé les renseignements personnels.*

☐ **Les renseignements sont privés, mais peu sensibles :** *ex : résultat académique, numéro de cellulaire, date de naissance.*

☐ **Les renseignements sont privés et peu sensibles, mais une fois jumelés avec d'autres renseignements, ils deviennent sensibles**

☐ **Les renseignements sont privés et sensibles :** *ex : numéro d'élève, numéro de carte de crédit.*

☐ **Les renseignements sont privés et très sensibles :** *de leur nature, notamment médicale, biométrique ou autrement intime, ou en raison du contexte de leur utilisation ou communication, ils suscitent un haut degré d'attente raisonnable en matière de respect de la vie privée.*

☐ **Autres,** précisez

Commentaires :

Il est possible d'expliquer brièvement vos conclusions quant au degré de sensibilité des renseignements concernés à la section commentaire.

5. Quelles sont les conséquences appréhendées ou possibles de l'utilisation des renseignements personnels?

- ☐ Fraude, perte financière ou impact sur le dossier de crédit;
- ☐ Dommages moraux (atteinte à la réputation, humiliation, atteinte à la vie, privée, diffamation, discrimination);
- ☐ Vol ou usurpation d'identité;
- ☐ Perte d'emploi ou impact sur le milieu de travail ou les relations professionnelles;
- ☐ Répercussions sur la santé physique ou psychologique;
- ☐ Problème de nature administrative;
- ☐ **Autres**, précisez

Commentaires :

Il est possible d'expliquer brièvement vos conclusions quant aux conséquences appréhendées ou possibles à la section commentaire.

6. Quelles sont les mesures prises pour éviter ou diminuer les risques qu'un préjudice soit causé?

☐ La pratique a été cessée ou a été modifiée;

☐ Les renseignements personnels ont été récupérés;

☐ Les renseignements personnels ont été détruits par le tiers; si oui, est-ce qu'une confirmation du tiers a été obtenue (verbalement, par écrit, etc.), précisez :

☐ Les lacunes informatiques ont été corrigées;

☐ Des tiers ont été informés, ce qui a permis de diminuer le risque de préjudice;

☐ Les mots de passe ou code d'accès ont été révoqués ou modifiés;

☐ **Autre,** précisez :

Commentaires :

Il est possible d'indiquer brièvement les mesures prises pour éviter ou diminuer les risques ainsi que le moment où ces mesures ont été prises à la section commentaire.

7. Quelles sont les probabilités que les renseignements concernés soient utilisés à des fins préjudiciables?

☐ **Nulle** : *L'incident n'aura raisonnablement aucune incidence ou les renseignements étaient protégés par un mot de passe ou étaient chiffrés;*

☐ **Faible** : *L'utilisation des renseignements ne mène pas à des conséquences sévères ou il est peu probable que les renseignements soient utilisés par la personne qui les a obtenues;*

☐ **Moyenne :** *L'utilisation des renseignements mènera des conséquences importantes et il est probable que les renseignements seront utilisés par la personne qui les a obtenus* ou nous ne sommes pas en mesure de déterminer les probabilités que les renseignements soient utilisés;

☐ **Élevée** : *L'utilisation des renseignements mènera des conséquences très importantes et il est presque certain que les renseignements seront utilisés par la personne qui les a obtenus;*

☐ **Autre**, précisez :

Commentaires :

Il est possible d'expliquer brièvement vos conclusions quant aux probabilités d'utilisation des renseignements concernés à la section commentaire.

8. Consultation du responsable de la protection des renseignements personnels *(L'article 63.10 de la LAI exige que le responsable de la protection des renseignements personnels soit consulté)*

Date de consultation	

9. Résultat de l'évaluation (présence ou non d'un préjudice sérieux soit un acte ou à un évènement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable.)

Nom de la personne qui a complété l'évaluation

Date

Démarches à effectuer en fonction des résultats de l'évaluation

Prochaines démarches à effectuer :

	OUI	NON	DATE
Inscription de l'incident au registre :	☐	☐	_____
Aviser la CAI, le cas échéant :	☐	☐	_____
Aviser la ou les personnes concernées :	☐	☐	_____
Aviser les tiers, le cas échéant :	☐	☐	_____
Mise en place ou poursuite de travaux :	☐	☐	_____
Autre : précisez :	☐	☐	_____

Description des travaux si nécessaire

Mise en garde

Cette grille d'évaluation du préjudice a été construite afin de tenir compte des obligations découlant de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Il est toutefois possible que l'organisation doive se conformer à d'autres obligations, notamment celle prévue en vertu de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ c. G-1.03). Il sera donc nécessaire d'en tenir compte dans le cadre de la présente évaluation.

AIDE MÉMOIRE CONCERNANT LES AUTRES DÉMARCHES À EFFECTUER EN LIEN AVEC LES RÉSULTATS DE L'ÉVALUATION

Dois-je inscrire l'incident au registre des incidents?

Oui, dès qu'un incident de confidentialité survient (peu importe la gravité du préjudice), celui-ci doit être consigné dans le registre des incidents.

Dois-je aviser la Commission d'accès à l'information?

Si l'incident présente un risque qu'un préjudice sérieux soit causé aux personnes dont les renseignements sont concernés, il est obligatoire d'aviser la CAI dès que possible. La grille d'évaluation sert à déterminer si l'incident présente un risque de préjudice sérieux.

Vous pouvez aviser la CAI par le biais du formulaire à compléter, disponible en ligne, sur le site internet de la CAI :

https://www.cai.gouv.qc.ca/documents/CAI_FO_avis_incident_confidentialite.pdf

Dois-je aviser les personnes concernées par les renseignements personnels qu'il y a eu un incident de confidentialité?

Si l'incident de confidentialité présente un risque de préjudice sérieux, il est obligatoire de le faire, **sauf si** cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois. Une fois qu'il a été déterminé qu'il n'y avait plus d'entrave, les personnes doivent être avisées.

Puis-je aviser un tiers qui est susceptible d'aider l'organisation à diminuer le risque de préjudice?

Si cela est susceptible de diminuer le risque de préjudice, **vous pouvez aviser des tiers**, et ce, peu importe la gravité du préjudice. Seuls les renseignements personnels qui sont nécessaires à pour diminuer le risque de préjudice peuvent être communiqués sans le consentement des personnes concernées.

Centre de services scolaire de Montréal
Québec
Bureau des affaires juridiques

AIDE-MÉMOIRE
Directive relative aux règles encadrant la gouvernance du CSSDM à l'égard des renseignements personnels

Principe directeur : Le CSSDM reconnait qu'il est **responsable des renseignements personnels** (RP) qu'il détient aux fins de l'accomplissement de sa mission et il entend prendre les mesures requises pour respecter la vie privée des personnes concernées.

Qu'est-ce qu'un renseignement personnel? Il s'agit d'un renseignement qui concerne une personne et qui permet de l'identifier de façon directe ou indirecte (ex.: les coordonnées de l'élève, le nom de ses parents, son état de santé, les services qui lui sont offerts, le dossier disciplinaire d'un employé, etc.).

Mesures de protection applicables à chaque étape du cycle de vie des renseignements personnels

- Ne **collecter** que les RP nécessaires pour atteindre des fins déterminées en lien avec l'exercice des fonctions du CSSDM (ex : ouvrir un compte, traiter une demande d'inscription, etc.)
- Lors de la **collecte**, informer la personne des fins de celle-ci
- Ne pas **utiliser** les RP à d'autres fins que celles identifiées lors de la collecte
- Ne pas **communiquer** des RP à une personne qui ne détient pas les autorisations requises
- Un employé peut avoir **accès** à un RP sans le consentement de la personne concernée, lorsqu'il a la qualité pour le recevoir et que ce RP est nécessaire à l'exercice de ses fonctions
- En respectant les modalités applicables, un employé peut **communiquer** des RP sans le consentement de la personne concernée, notamment:
  - Dans le cadre de l'exécution d'un contrat de services ou d'entreprise
  - Lorsque requis par un service de police, par la DPJ ou par un organisme ayant le pouvoir de contraindre à leur communication
  - Pour prévenir un acte de violence, dont un suicide
- Connaitre et appliquer les **mesures de sécurité** déterminées par le CSSDM pour protéger les RP, qu'ils soient conservés en format papier ou électronique
- S'assurer de l'exactitude des RP **conservés** afin qu'ils puissent servir aux fins déterminées.
- Appliquer le calendrier de conservation du CSSDM ou **détruire** de façon sécuritaire les RP lorsque les fins pour lesquelles ils ont été collectés sont accomplies

Collecte

Utilisation

Communication

Conservation

Destruction

Gestion des consentements

Lorsque requis pour la collecte, l'utilisation et la communication d'un RP, le consentement de la personne doit être :

- **Manifeste :** Évident et donné d'une façon qui démontre la volonté réelle de la personne. Lorsque possible et dans le cas d'un RP sensible, le consentement devrait être obtenu de façon expresse, c'est-à-dire explicitement exprimé par un geste témoignant de l'acceptation de la personne
- **Libre :** impliquant un choix réel et donné sans contrainte ni pression
- **Éclairé :** donné en connaissance de cause par le biais de termes simples et clairs
- **Spécifique :** donné dans un objectif précis pour chaque fin et valide seulement pour la durée nécessaire

Principes

1. Aider la personne à comprendre la portée du consentement
2. Obtenir le consentement de la bonne personne et vérifier la qualité du représentant légal (pour les élèves de moins de 14 ans)
3. Conserver la preuve du consentement
4. En cas de retrait du consentement, informer la personne des conséquences de ce retrait

Mesures de protection particulières lors d'un sondage

Sont visés : tous les sondages visant la collecte de RP (sondages d'opinion, de satisfaction, entrevue individuelle ou de groupe, sondages automatisés de type FORMS, etc.)

Principes

1. Évaluer la nécessité de recourir à un sondage (lien avec la mission CSSDM). Les sondages n'impliquant pas la collecte de RP sont favorisés
2. Planifier le sondage : établir l'objectif, procéder à une évaluation de l'aspect éthique, identifier les RP collectés, les personnes qui y auront accès, leur lieu de conservation, leur durée de conservation, etc.
3. Obtenir l'autorisation de la direction de l'Unité administrative concernée
4. Sondages de type FORMS : une fois les RP transférés dans leur lieu de conservation, ils doivent être supprimés du lieu de production
5. La publication des résultats d'un sondage ne doit pas permettre d'identifier directement ou indirectement les participants

Rôles et responsabilités des employés

- Prendre connaissance et respecter la Directive
- Participer aux formations et utiliser les modèles et outils mis à sa disposition
- Collaborer dans le cadre d'une demande d'accès aux documents, une demande de rectification d'un RP, lors du traitement d'une plainte ou d'un incident de confidentialité
- Communiquer avec son supérieur pour obtenir des précisions, des conseils ou pour l'informer d'une problématique en lien avec un cas particulier

Incident de confidentialité

Déclarer **sans délai** les incidents de confidentialité impliquant une communication, une utilisation ou un accès non autorisé à un RP ou la perte d'un tel renseignement à la Responsable de la protection des RP à l'adresse : accesdoc@cssdm.gouv.qc.ca.

Plaintes en lien avec les RP

Écrivez à accesdoc@cssdm.gouv.qc.ca