Comité de gestion de la taxe scolaire
DE L'ÎLE DE MONTRÉAL

POLITIQUE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

(Adoptée par le Comité de gestion de la taxe scolaire de l'île de Montréal le 15 septembre 2022 par la résolution 6)

---

1. PRÉAMBULE

La Politique sur la protection des renseignements personnels découle du cadre général régissant l'utilisation des actifs informationnels du Comité de gestion. Elle permet au Comité de gestion d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'elle a créée ou reçue.

L'information liée aux ressources humaines, matérielles, technologiques et financières est accessible sur des formats numériques et non-numériques. Les risques d'atteinte à la disponibilité, intégrité ou confidentialité de ces informations peuvent avoir des conséquences liées à :

- L'atteinte à la protection des renseignements personnels et à la vie privée;
- La prestation de services à la population;
- La réputation du Comité de gestion.

2. CONTEXTE

La loi 25 modernise les dispositions législatives en matière de protection des renseignements personnels. Elle vise à répondre aux préoccupations croissantes des citoyennes et des citoyens en cette matière, par une protection accrue de la vie privée en tenant compte des réalités technologiques actuelles.

Elle permet d'actualiser l'encadrement applicable à la protection des renseignements personnels dans diverses lois dont la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

Le Comité de gestion est désormais tenu d'adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique de protection des renseignements personnels en ayant recours notamment à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

Tel que requis par la loi, un responsable de l'accès aux documents et un responsable de la protection des renseignements personnels sont désignés par le directeur général du Comité de gestion.

2.1 Comité sur l'accès à l'information et la protection des renseignements personnels (ci-après appelé « le comité »)

Toujours pour répondre aux exigences de la loi, le directeur général du Comité de gestion procède à la nomination des membres du Comité sur l'accès à l'information et la protection des renseignements personnels. Ce comité est composé :

- un responsable de l'accès aux documents
- un responsable de la protection des renseignements personnels
- un responsable de la gestion documentaire

Le comité veillera à soutenir les personnes responsables de l'accès et de la protection des renseignements personnels dans l'exercice de leurs responsabilités et dans l'exécution de leurs obligations.

Le comité a aussi pour fonction d'approuver les règles de gouvernance sur l'accès à l'information et la protection des renseignements personnels.

Enfin, il a pour rôle d'évaluer les facteurs à la vie privée de tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

3. DÉFINITIONS

Renseignement personnel sensible :

L'article 59 de la Loi définit « renseignement personnel sensible » de la manière suivante : « Pour l'application de la présente Loi, un renseignement personnel est sensible lorsque, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée».

Le consentement :

Les exigences relatives au consentement sont prévues à l'article 53.1 de *la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels :*

- Il doit être manifeste, libre, éclairé, être donné à des fins spécifiques et limité à sa durée nécessaire;

- En termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée;
- Si la personne le requiert, il faut prêter assistance pour l'aider à comprendre la portée du consentement demandé.

Incidents de confidentialité :

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* nous renseigne sur ce que peut constituer un incident de confidentialité :

- L'accès non autorisé par la loi à un renseignement personnel;
- L'utilisation non autorisée par la loi d'un renseignement personnel;
- La communication non autorisée par la loi d'un renseignement personnel;
- La perte d'un renseignement personnel ou toute atteinte à la protection d'un tel renseignement.

4. OBJECTIFS

Par cette politique, le Comité de gestion affirme son engagement à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information mais plus particulièrement de la protection des renseignements personnels, quel que soit son support ou ses moyens de communication. À cet égard, le Comité de gestion doit veiller à :

- La **disponibilité** de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;

- L**'intégrité** de l'information de manière à ce que celle-ci ne soit ni détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;

- La **confidentialité** de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.

5. CADRE LÉGAL ET ADMINISTRATIF

La présente politique s'inscrit, entre autres, dans les contextes législatifs suivant :

- La Charte des droits et libertés de la personne (LRQ, chapitre C- 12);
- La *Loi sur l'instruction publique* (L.R.Q. c. l-13.3);

- La *Loi sur les archives* (L.R.Q. c. A-21.1);
- Le Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (L.R.Q. c. A-21.1, r.1);
- Le Code civil du Québec (LQ, 1991, chapitre 64);
- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, Loi 133);
- La *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A- 2.1);
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2);
- La Directive sur la sécurité de l'information gouvernementale;
- Les Règlements, politiques, procédures et autres encadrements administratifs du Comité de gestion.

6. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs de l'information du Comité de gestion, c'est-à-dire, tout son personnel, quel que soit son statut, les membres du Comité de gestion, toute personne physique ou morale qui, à titre de partenaire, consultant, fournisseur ou visiteur, utilise ou a accès aux actifs informationnels et plus spécifiquement aux renseignements personnels du Comité de gestion.

L'information visée est celle que le Comité de gestion détient dans le cadre de ses activités, fonctions, pouvoirs et mission, quelle que soit sa nature ou le support utilisé, que sa conservation soit assurée par lui-même ou par un tiers.

7. PRINCIPES DIRECTEURS

Les principes directeurs qui guident les actions du Comité de gestion en matière de protection des renseignements personnels sont les suivants :

- S’assurer de bien connaître l’information à protéger, en identifier les détenteurs et leurs caractéristiques de sécurité;

- Reconnaître l’importance de mieux encadrer la gouvernance à l’égard des renseignements personnels et d’instaurer une politique sur la protection des renseignements personnels;

- Reconnaître l’importance de diffuser la politique et les activités de formation et de sensibilisation qui s’y rattachent auprès de tous les employés du Comité de gestion et de publier la politique et une description des activités de formation sur son site Web;

- Reconnaître les rôles et responsabilités de tous et chacun pour protéger l'information tout au long de son cycle de vie (création, traitement, destruction).

8. CATÉGORISATION DES ACTIFS INFORMATIONNELS

Le Comité de gestion a procédé à une catégorisation des actifs informationnels qui permet de soutenir une analyse de risques et permet d’évaluer la valeur de l’information à protéger. Il peut, par la suite, justifier les mesures de sécurité à mettre en œuvre et à les appliquer afin de fournir un niveau adéquat de sécurité.

Cette catégorisation, sous forme de grille, nous sert d’inventaire des renseignements personnels. La grille couvre tous les secteurs d’activités pour chacun des départements du Comité de gestion. On peut y retrouver le type d’information, son support, papier ou disque, le détenteur de l’information, et sa classification, privée ou publique.

Une classification par grade de risque doit être établie pour la disponibilité de l’information, son intégrité et la confidentialité. Un exercice doit être réalisé pour bien identifier la sévérité du risque relativement aux différents actifs informationnels. Les renseignements personnels que nous détenons sont identifiés tout comme l’endroit où ils sont stockés. De par cet exercice, nous pouvons assurer un meilleur contrôle de nos informations et cibler davantage nos mesures de sécurité pour réduire au maximum la survenance d’incidents de confidentialité.

Le niveau de protection de l’information est établi en fonction :

- De la nature de l’information et de son importance;
- Des probabilités d’accident, d’erreur ou de malveillance auxquelles elles sont exposées;
- Des conséquences de la matérialisation de ces risques.

La mise à jour de la grille des actifs informationnels doit être faite annuellement.

Le comité sur l'accès à l'information et à la protection des renseignements personnels a procédé à une revue complète de la grille de catégorisation des actifs informationnels du Comité de gestion pour identifier les secteurs d'activités du Comité de gestion où l'on retrouve des renseignements personnels et pour lesquels des mesures spécifiques sont instaurées mais qui seront revues périodiquement pour éviter la survenance de tout incident. Nous avons identifié les secteurs d'activité du Comité de gestion les plus à risques :

- Gestion de la paie où l'on retrouve différents types de renseignements personnels;

- Formulaires d'absence, budget rémunération, analyses, etc.;

- Service de la taxation incluant l'encaissement, les ajustements, remboursements, recouvrement et service clientèle. Plusieurs demandes concernant des relevés de taxes chaque année provenant de citoyens;

- Régime de gestion des risques (RGR), fonds d'auto-assurance, cas judiciarisés, procès-verbaux du Comité du RGR, banque de données des réclamations, rapports d'événement et d'enquête;

- Activités reliées aux écoles en milieux défavorisés (EMD) : Par sa mission, le Comité de gestion assure la redistribution des surplus de la taxe scolaire en faveur des mesures de rattrapage dans les écoles en milieux défavorisés. Cette opération se fait suivant une base de données renfermant de nombreux renseignements que l'on doit considérer « sensibles ».

Pour tous ces secteurs d'activités, le grade de risque au niveau de la confidentialité des renseignements est au plus élevé.

9. GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Le Comité de gestion déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires à l'obtention des buts suivants :

- Limiter l'occurrence des incidents en matière de protection des renseignements personnels;
- Gérer adéquatement ces incidents pour en minimiser les conséquences;
- S'assurer de mettre en place les mécanismes pour éviter que de nouveaux incidents de même nature ne se produisent.

Les incidents présentant un risque qu'un préjudice sérieux soit causé sont déclarés à la Commission d'accès à l'information du Québec.

Ils sont aussi déclarés à la personne concernée, à moins que cela soit susceptible d'entraver une enquête en cours.

Le Comité de gestion maintient un registre des incidents de confidentialité.

10. PROCESSUS DE TRAITEMENT DES PLAINTES

Toute plainte relative à un incident de confidentialité est dirigée au Secrétariat général pour y être administrée. Dans le cas d'une plainte visant un membre du Comité de gestion, la plainte devra être adressée à l'attention du Responsable de l'éthique et de déontologie via le Secrétariat général.

- La plainte doit être déposée par écrit et comporter une description de l'incident, la date ou la période où l'incident s'est produit, la nature des renseignements personnels visée par l'incident et le nombre de personnes concernées;

- Le Secrétariat général analysera la plainte en prenant pour compte notamment la sensibilité du renseignement, les conséquences appréhendées et la probabilité de l'utilisation à des fins préjudiciables;

- S'il y a des motifs de croire que s'est produit un incident de confidentialité, le Secrétariat général verra à établir les circonstances de l'incident, cibler les renseignements personnels, les personnes visées et la nature du problème;

- Il déterminera la nature du préjudice en collaboration avec la personne responsable des renseignements personnels;

- Si à l'issu de l'analyse de la plainte, il y a risque de préjudice sérieux, le Secrétariat général verra à aviser la Commission de l'accès à l'information et les personnes concernées sauf dans ce dernier cas, si un tel avis peut entraver une enquête en cours menée par une personne ou organisme chargé de réprimer le crime;
- Procède à l'inscription de l'incident de confidentialité au registre;

- Mise en place de mesures de mitigation afin de réduire les préjudices liés à l'incident et éviter qu'un tel incident ne se reproduise.

Advenant le cas où la plainte met en cause le secrétaire général, cette dernière devra être adressée à l'attention du directeur général.

11. SENSIBILISATION ET FORMATION

La protection des renseignements personnels repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, le personnel du Comité de gestion doit être formé et sensibilisé à : la sécurité de l'information et des systèmes

d'information du Comité de gestion; aux directives de la sécurité; à la gestion des risques; à la gestion des incidents de confidentialité ; aux menaces existantes; aux conséquences d'une atteinte à la sécurité et à leur rôle et à leurs responsabilités en la matière.

Des activités de sensibilisation et de formation sont offertes de façon continue.

Un calendrier d'activités a été déployé. Par le biais de capsules quiz nous pourrons assurer de la bonne compréhension par tous des enjeux liés à la protection des renseignements personnels. Des capsules spécifiquement conçues telles « Les éléments clés de la réforme » ainsi que « Les droits des individus et la protection de leurs renseignements personnels » et « Les obligations des entreprises » sont présentées à date fixe mais seront aussi disponibles en tout temps sur le site du Comité de gestion. Des quiz avec note de passage pour chacune des capsules nous assurent de la compréhension de tous et chacun. Chaque employé est tenu de réussir le test pour compléter cette formation obligatoire.

Les incidents de confidentialités peuvent résulter d'un geste volontaire ou involontaire commis par une personne de l'interne ou de l'externe. Parmi les incidents de confidentialité les plus fréquents, on retrouve entre autre :

- L'hameçonnage
- Le déploiement de logiciels malveillants
- Les rançongiciels
- L'envoi de renseignements personnels à la mauvaise adresse courriel

Toujours de manière à prévenir les incidents de confidentialité, des capsules de formation relatives à l'hameçonnage, les rançongiciels, les courriels et les logiciels malveillants sont aussi ajoutées au calendrier de formation.

Une description des activités de formation est disponible sur le site Web du Comité de gestion.

12. SANCTIONS

Tout employé ou membre du Comité de gestion qui contrevient à la présente politique s'expose à des mesures disciplinaires (incluant le congédiement), administratives ou légales.

13. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le responsable de l'accès aux documents, assisté du comité sur l'accès à l'information et la protection des renseignements personnels, s'assure de la diffusion et de la mise à jour de la politique sur le site Web du Comité de gestion.

14. RESPONSABILITÉ DE L'APPLICATION ET RÉVISION DE LA POLITIQUE

Le secrétaire général est responsable de l'application de la politique et de sa révision.

La Politique sur la protection des renseignements personnels pourra être révisée lors de changements significatifs mais devra obligatoirement être révisée dans les 2 ans de son adoption.

15. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption.