Centre de services scolaire des Hautes-Laurentides
Québec

SG-2024-28

☐ Règlement
☐ Politique (cadre, code)
☒ Procédure (directive, guide, référentiel)

DIRECTIVE SUR LES RÔLES ET RESPONSABILITÉS EN CAS D'INCIDENTS DE CONFIDENTIALITÉ

Approbation :	Direction générale
Responsable :	Direction du secrétariat général, des communications et du transport
Date d'approbation :	2024-08-19
Date d'entrée en vigueur :	2024-08-19
Date prévue de révision :	Au besoin

Liste des écrits de gestion remplacés :
N/A

Ce document a été rédigé en respectant les règles de la nouvelle orthographe de l'Office de la langue française.

TABLE DES MATIÈRES

1. CADRE JURIDIQUE

La présente directive découle des articles 63.8 à 63.11 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 « LAI »).

La présente directive doit être lue en concordance avec les différents outils existant au Centre de services scolaire des Hautes-Laurentides (ci après «CSSHL») concernant la protection des renseignements personnels.

2. BUT ET OBJECTIFS DE LA DIRECTIVE

Le but de la directive est d'assurer la mise en œuvre des obligations du CSSHL découlant de la LAI en lien avec les incidents de confidentialité.

Les objectifs de la directive sont les suivants :

- Énoncer les principes sur lesquels repose la protection des renseignements personnels recueillis, utilisés, communiqués et conservés dans le cadre de l'exercice des fonctions du CSSHL;
- Établir un processus de déclaration des incidents de confidentialité pouvant survenir dans le cadre des fonctions du CSSHL;
- Informer les membres du personnel et autres personnes du CSSHL sur les incidents de confidentialité;
- Déterminer les rôles et responsabilités des personnes visées par la présente directive.

3. CHAMP D'APPLICATION

La présente directive s'applique à l'ensemble du personnel du CSSHL (écoles, centres, services). Elle s'applique également aux membres du conseil d'administration, aux membres des conseils d'établissements et aux membres des différents comités du CSSHL.

La présente directive n'a pas pour effet de limiter les responsabilités du CSSHL découlant de sa *Politique de sécurité de l'information* [SG-20] adoptée 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) des règlements et des directives qui en découlent.

4. DÉFINITIONS

Les termes utilisés dans la présente directive sont ceux de la LAI et des autres encadrements légaux applicables, sauf indication contraire.

Pour faciliter la compréhension de la présente directive, on entend par :

Comité AIPRP	Le comité sur l'accès à l'information et la protection des renseignements personnels du CSSHL
Déclarant	Personne qui a connaissance d'un possible incident de confidentialité
Incident de confidentialité	**1.** L'accès non autorisé par la loi à un renseignement personnel **2.** L'utilisation non autorisée par la loi d'un renseignement personnel **3.** La communication non autorisée par la loi d'un renseignement personnel **4.** La perte d'un renseignement personnel **5.** Toute autre atteinte à la protection d'un tel renseignement
Personne	Une personne visée par le champ d'application de la présente directive agissant au nom du CSSHL ou dans le cadre de ses fonctions
Renseignement personnel	Renseignements qui concernent une personne physique et permettent directement ou indirectement de l'identifier
Responsable	Personne désignée comme Responsable de la protection des renseignements personnels du CSSHL

5. PRINCIPES GÉNÉRAUX

5.1. Une Personne doit recueillir uniquement les renseignements personnels nécessaires aux fonctions du CSSHL.

5.2. Une Personne a accès uniquement aux renseignements personnels qui sont nécessaires à l'exercice de ses fonctions.

5.3. Une Personne ne peut communiquer des renseignements personnels sans le consentement de la personne concernée, de son représentant, ou dans les cas prévus par la loi.

5.4. Une Personne qui a connaissance d'un incident de confidentialité doit le déclarer dans les plus brefs délais en conformité de la présente directive.

6. PROCESSUS LORS D'UN INCIDENT DE CONFIDENTIALITÉ

6.1. DÉCLARATION D'UN INCIDENT DE CONFIDENTIALITÉ

6.1.1. Le Déclarant doit, sans délai, informer la direction de son unité administrative (école, centre, service) de tout événement pouvant laisser croire qu'il s'est produit un incident de confidentialité.

6.1.2. Dans la mesure du possible, le Déclarant fournit les informations suivantes relativement à l'incident de confidentialité :

- Le contexte et les circonstances entourant l'événement (Date, description des faits survenus, etc.);
- La nature des renseignements personnels concernés (par exemple : noms, adresse, courriel, code permanent, etc.);
- Le fait que ces renseignements étaient ou non protégés par un mot de passe ou un code d'accès, par exemple;
- Le nombre de personnes concernées par les renseignements personnels;
- L'identité et le nombre de personnes ou l'organisme qui ont reçu les renseignements personnels, le cas échéant;
- Les mesures immédiates prises, le cas échéant;
- Toute autre information pertinente.

6.1.3. Le Déclarant et la direction doivent, dès que possible, poser les gestes nécessaires qui diminueraient les risques qu'un préjudicie soit causé (rappel d'un courriel; téléphone, etc.).

6.1.4. La direction doit sans délai informer le Responsable de la protection des renseignements personnels de l'évènement qui lui a été dénoncé et lui transmettre les informations pertinentes.

6.2. ANALYSE DE LA SITUATION DÉNONCÉE

6.2.1. Le Responsable analyse la situation dénoncée.

6.2.2. Au besoin, il obtient des informations supplémentaires.

6.2.3. Il statue sur la situation et détermine s'il s'agit d'un incident de confidentialité.

6.2.4. 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'évènement, il communique avec la direction afin qu'elle pose, le cas échéant, les gestes appropriés.

6.3. TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

6.3.1. Le Responsable s'assure que les gestes ou les mesures, qui sont susceptibles de diminuer les risques qu'un préjudicie soit causé aux personnes dont les renseignements personnels sont concernés par l'incident de confidentialité, soient mis en œuvre en tenant compte de ceux qui ont été posés par le Déclarant ou la direction, le cas échéant.

Il pourrait s'agir, par exemple :

6.3.1.1 Obtenir des personnes, à qui ont été illégalement communiqués des renseignements personnels, une confirmation de destruction des renseignements personnels obtenus;
6.3.1.2 Obtenir des personnes, à qui ont été illégalement communiqués des renseignements personnels, un engagement de non-divulgation des renseignements personnels obtenus;
6.3.1.3 Recommander une intervention auprès des employés concernés.

6.3.2. Le Responsable évalue le risque de préjudice sérieux de l'incident de confidentialité en considérant notamment la sensibilité du renseignement, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables (voir annexe 2).

6.3.3. Si l'incident de confidentialité présente un risque sérieux, le Responsable doit :

- Aviser la Commission d'accès à l'information avec diligence, de la manière et en fournissant les informations requises par le règlement applicable (voir annexe et formulaire en ligne FORMULAIRE DE DÉCLARATION 19-09-2022 VFin (gouv.qc.ca));
- Aviser toute personne dont les renseignements personnels sont concernés par l'incident de confidentialité de la manière et en fournissant les informations requises par le règlement applicable (voir annexe 1);
- 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 vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois;
- Aviser toute personne ou tout organisme susceptible de diminuer le risque de préjudice sérieux (ministère, police, etc.) en ne communiquant que les renseignements personnels nécessaires à cette fin et inscrire cette communication au registre des communications en vertu de la LAI.

6.3.4. Le Responsable inscrit l'incident au registre des incidents de confidentialité dans tous les cas.

6.4. MESURES À PRENDRE POUR ÉVITER QU'UN INCIDENT DE CONFIDENTIALITÉ DE MÊME NATURE SE REPRODUISE

6.4.1. Une fois les mesures immédiates accomplies, le Responsable détermine si d'autres mesures devraient être appliquées pour éviter que d'autres incidents de même nature ne se reproduisent.

Il pourrait s'agir, par exemple :

6.4.1.1 La modification des accès informatiques;
6.4.1.2 La suppression de renseignements personnels;
6.4.1.3 La mise en place de formation ou autres mesures de sensibilisation;
6.4.1.4 La révision de processus internes (logiciels, méthodes de travail, etc.).

7. COMITÉ AIPRP

7.1. Le Responsable peut en tout temps consulter le Comité AIPRP du CSSHL dans l'analyse et le traitement d'une situation pouvant être un incident de confidentialité.

7.2. Le Responsable fait rapport annuellement au Comité AIPRP des incidents de confidentialité survenus et des mesures mises en place.

7.3. Dans tous les cas, il transmet au Comité AIPRP les recommandations de la Commission d'accès à l'information, le cas échéant.

8. INFORMATION ET DIFFUSION

8.1. Le Responsable s'assure de la diffusion de la présente directive auprès des différentes unités administratives.

8.2. Au besoin, en collaboration avec les directions, le Responsable s'assure qu'une formation adéquate soit disponible et offerte aux membres du personnel.

9. ENTRÉE EN VIGUEUR

La présente directive entre en vigueur à la date de son approbation.

Outil développé en collaboration avec la Fédération des Centres de services scolaires du Québec, la Table des secrétaires généraux des Commissions scolaires anglophones du Québec et Morency, société d'avocats S.E.N.C.R.L. (2023).

ANNEXE I

Extraits du Règlement sur les incidents de confidentialité, publié dans le Décret 1761-2022 du 30 novembre 2022, dans la Gazette officielle du Québec du 14 décembre 2022, 154e année, no 50, p. 6819.

AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION

3. L'avis à la Commission d'accès à l'information qu'un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé, donné en application du deuxième alinéa de l'article 63.8 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1) ou du deuxième alinéa de l'article 3.5 de *la Loi sur la protection des renseignements personnels dans le secteur privé* (chapitre P-39.1), est fait par écrit et doit contenir les renseignements suivants:

1° le nom de l'organisation ayant fait l'objet de l'incident de confidentialité et, le cas échéant, le numéro d'entreprise du Québec qui lui est attribué en vertu de la *Loi sur la publicité légale des entreprises* (chapitre P-44.1);

2° le nom et les coordonnées de la personne à contacter au sein de l'organisation relativement à l'incident;

3° une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;

4° une brève description des circonstances de l'incident et, si elle est connue, sa cause;

5° la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

6° la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;

7° le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres;

8° une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, telles la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;

9° les mesures que l'organisation a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, en application du deuxième alinéa de l'article 63.8 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ou du deuxième alinéa de l'article 3.5 de *la Loi sur la protection des renseignements personnels dans le secteur privé*, de même que la date où les personnes ont été avisées ou le délai d'exécution envisagé;

10° les mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que la date ou la période où les mesures ont été prises ou le délai d'exécution envisagé;

11° le cas échéant, une mention précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.

4. L'organisation doit transmettre à la Commission d'accès à l'information tout renseignement énoncé à l'article 3 dont elle prend connaissance après lui avoir transmis l'avis qui y est visé. L'information complémentaire doit alors être transmise avec diligence à compter de cette connaissance.

CONTENU DE L'AVIS À LA PERSONNE DONT UN RENSEIGNEMENT PERSONNEL EST CONCERNÉ

1. L'avis à la personne dont un renseignement personnel est concerné par un incident qui présente un risque qu'un préjudice sérieux soit causé, donné en application du deuxième alinéa de l'article 63.8 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1) ou du deuxième alinéa de l'article 3.5 de la *Loi sur la protection des renseignements personnels dans le secteur privé* (chapitre P-39.1), doit contenir les renseignements suivants:

1° une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;

2° une brève description des circonstances de l'incident;

3° la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

4° une brève description des mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;

5° les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;

6° les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

CIRCONSTANCES SELON LESQUELLES L'AVIS À LA PERSONNE EST TRANSMIS PAR AVIS PUBLIC

6. L'avis visé à l'article 5 est transmis à la personne concernée par l'incident de confidentialité.

Malgré le premier alinéa, l'avis visé à l'article 5 est donné au moyen d'un avis public dans l'une ou l'autre des circonstances suivantes:

1° lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée;

2° lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'organisation;

3° lorsque l'organisation n'a pas les coordonnées de la personne concernée.

Par ailleurs, afin d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou afin d'atténuer un tel préjudice, l'avis visé à l'article 5 peut également être donné au moyen d'un avis public. Dans ce cas, l'organisation demeure toutefois tenue de transmettre, avec diligence, un avis à la personne concernée, à moins que l'une des circonstances énoncées au deuxième alinéa ne s'applique à sa situation.

En application du présent article, un avis public peut être fait par tout moyen dont on peut raisonnablement s'attendre à ce qu'il permette de joindre la personne concernée.

ANNEXE II

GRILLE D'ÉVALUATION DU RISQUE DE PRÉJUDICE SÉRIEUX

La grille permet d'établir le niveau de préjudice et de documenter la démarche.

1. Date ou période de l'événement :

_____

2. Type d'incident / cause de l'incident :

☐ Accès non autorisé;
☐ Utilisation non autorisée;
☐ Communication non autorisée;
☐ Perte ou autre atteinte à la protection des renseignements personnels.

3. Est-ce que des renseignements personnels sont concernés?

☐ Oui, il s'agit d'un incident de confidentialité (veuillez remplir les questions subséquentes pour évaluer les risques de préjudice);
☐ Non, il s'agit d'un incident de sécurité (veuillez inscrire l'incident au registre des incidents de sécurité, en informer le responsable de la sécurité et continuer l'analyse pour évaluer les conséquences appréhendées et les mesures à prendre).

4. Quelle est la nature des renseignements personnels concernés?

☐ Renseignements d'identification (nom, coordonnées, adresse postale, courriel, numéro de téléphone, numéro d'assurance sociale/maladie, permis de conduire, passeport, code permanent, code d'utilisateur, mot de passe, etc.);
☐ Renseignements financiers (numéro de carte de crédit ou de compte bancaire, salaire, conditions d'emploi, etc.);
☐ Renseignements de santé (dossier médical, âge, taille, poids, plan d'intervention, groupe sanguin, etc.);
☐ Renseignements relatifs au travail (dossier disciplinaire, motifs d'absences, dates de vacances, salaire, évaluation du rendement, heures d'entrée et de sortie liées au lieu de travail, etc.);
☐ Renseignements génétiques ou biométriques (empreintes digitales, signature vocale, ADN, etc.);
☐ Autre (précisez) (combinaison de facteurs pouvant rendre les renseignements sensibles, dont les antécédents judiciaires, le dossier d'employé, etc.):

_____

5. Qui détient maintenant les renseignements personnels faisant l'objet de l'incident de confidentialité?

☐ Organisme public;
☐ Citoyen;
☐ Entreprise privée;
☐ Inconnu.

6. Quelles sont les probabilités que ces renseignements personnels soient utilisés à des fins préjudiciables?

☐ Nulles;
☐ Faibles;
☐ Moyennes;
☐ Élevées.

7. Quelles sont les conséquences appréhendées de l'utilisation malintentionnée de ces renseignements personnels?

☐ Vol ou usurpation d'identité;
☐ Fraude ou perte financière;
☐ Répercussion négative sur la santé physique ou psychologique;
☐ Perte d'emploi ou perte d'occasion d'emploi;
☐ Dommages moraux (humiliation, atteinte à la réputation ou à la vie privée, discrimination, diffamation);
☐ Autre (précisez):

_____

_____

_____

_____

☐ Aucune.

8. En fonction de cette évaluation, un risque de préjudice sérieux peut-il être appréhendé?

☐ Oui, continuez l'analyse;

☐ Non, vous n'avez pas à aviser la Direction de la surveillance de la CAI, mais vous devez inscrire l'incident au registre et prendre des mesures pour atténuer le risque de préjudice.

9. Quelles mesures ont été prises pour éviter ou réduire le risque qu'un incident de même nature se reproduise?

☐ Les renseignements personnels ont été récupérés et n'ont pas été consultés;

☐ L'appareil a été effacé à distance et les renseignements n'ont pas été consultés;

☐ Le problème à l'origine de la violation a été résolu;

☐ Les détenteurs des renseignements personnels ont été contactés;

☐ Autre (précisez) (correction des méthodes de travail, formation, mesures de sécurité administratives, physiques ou techniques, contact avec les autorités policières ou des experts externes, etc.) :

_____

_____

_____

_____

☐ Aucune.

10. Quelles sont les mesures mises en place pour empêcher l'accès aux renseignements personnels? (Ex. sécurisation de la clé de cryptage pour déverrouiller des renseignements personnels cryptés, authentification multifacteurs pour accéder à un compte, protection d'un document à l'aide d'un mot de passe, etc.):

_____

_____

_____

_____

11. Le responsable de l'accès doit toujours inscrire l'incident au registre des incidents de confidentialité, et l'incident doit, s'il présente un risque de préjudice sérieux (plus d'un choix peut s'appliquer) :

☐ Être déclaré avec diligence à la Direction de la surveillance en utilisant le formulaire d'avis de la Commission;

☐ Être communiqué à une personne ou à un organisme susceptible d'atténuer le préjudice*;

☐ Être déclaré aux personnes concernées**.

Note :

* La communication des renseignements sera faite sans le consentement de la personne concernée. La communication doit être inscrite dans le registre de communications des renseignements nécessaires.

** La personne concernée n'a pas à être avisée si cela est susceptible d'entraver une enquête menée par une personne ou un organisme qui, en vertu de la loi, est chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois. Dans le cas où un avis est nécessaire et que la personne n'est pas joignable ou qu'un tel avis ne lui cause un préjudice additionnel, la Commission peut aviser les personnes concernées au moyen d'un avis public.

Signature de la personne ayant fait l'évaluation : _____

Signature du responsable PRP : _____

Date de l'évaluation : _____

Source : Grille provenant de la Commission d'accès à l'information du Québec