Centre
de services scolaire
des Patriotes
Québec

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

Dernière mise à jour : 16 avril 2024

TABLE DES MATIÈRES

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).

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 »).

Elle doit être lue en concordance avec les orientations, encadrements ou autres outils en vigueur au Centre de services scolaire des Patriotes (ci-après « CSSP ») concernant la protection des renseignements personnel.

2 BUT ET OBJECTIFS

Le but de la directive est d'assurer la mise en œuvre des obligations du CSSP 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 CSSP;
- Établir un processus de déclaration des incidents de confidentialité pouvant survenir dans le cadre des fonctions du CSSP;
- Informer les membres du personnel et autres personnes du CSSP 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 CSSP (écoles, centres, services administratifs). Elle s'applique également aux membres du conseil d'administration, aux membres des conseils d'établissements et aux membres des différents comités du CSSP.

Elle n'a pas pour effet de limiter les responsabilités du CSSP découlant de sa politique de sécurité informationnelle 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 :

TERMES	DÉFINITIONS
Comité sur l'accès	Comité sur l'accès à l'information et la protection des renseignements personnels du CSSP composé de la responsable de l'accès aux documents et de la protection des renseignements personnels, de la coordonnatrice responsable de la gestion documentaire et de la Chef de la sécurité de l'information organisationnelle (CSIO).
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
Employé ou mandataire du CSSP	Une personne visée par le champ d'application de la présente directive, soit l'ensemble du personnel du CSSP (écoles, centres, services administratifs), les membres du conseil d'administration, les membres des conseils d'établissements et les membres des différents comités du CSSP, lorsqu'ils agissent au nom du CSSP ou dans le cadre de leurs fonctions.
Renseignements personnels	Renseignements qui concernent une personne physique et permettent directement ou indirectement de l'identifier (tel que défini à l'article 54 LAI)
Responsable	Personne désignée comme responsable de l'accès aux documents et de la protection des renseignements personnels, par la plus haute autorité conformément à la LAI.

5 PRINCIPES GÉNÉRAUX

Le CSSP s'engage à assurer la protection des renseignements personnels qui lui sont confiés, et ce, conformément à ses obligations et conformément à la *Directive relative aux règles encadrant la gouvernance des renseignements personnels* et au *Cadre de gestion de la sécurité de l'information*.

Un Employé ou mandataire doit recueillir uniquement les renseignements personnels nécessaires aux fonctions du CSSP.

Un Employé ou mandataire a accès uniquement aux renseignements personnels qui sont nécessaires à l'exercice de ses fonctions.

Un Employé ou mandataire ne peut communiquer des renseignements personnels sans le consentement de la personne concernée, de son représentant, ou dans les cas prévus par la LAI.

Un Employé ou mandataire 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

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

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 afin de limiter les impacts de l'incident, le cas échéant (rappeler le courriel, par exemple);
- Toute autre information pertinente.

Le Déclarant et la direction de l'unité administrative doivent, dès que possible, poser les gestes nécessaires qui diminueraient les risques qu'un préjudicie soit causé (rappel d'un courriel; appel à la personne concernée, etc.)

La direction et le Déclarant doivent compléter le formulaire en ligne afin de déclarer l'incident de confidentialité.

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

6.2 Analyse de la situation dénoncée

La Responsable analyse la situation dénoncée. Au besoin, elle obtient des informations supplémentaires.

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

Si elle détermine qu'il ne s'agit pas d'un incident de confidentialité, mais qu'elle juge qu'une intervention est tout de même nécessaire auprès des personnes impliquées dans l'événement, elle communique avec la direction afin qu'elle pose, le cas échéant, les gestes appropriés.

6.3 Traitement d'un incident de confidentialité

La 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 de l'unité, le cas échéant.

Par exemple, le Responsable pourrait :

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

La Responsable évalue le risque de préjudice sérieux de l'incident de confidentialité en considérant notamment la sensibilité des renseignements personnels concernés, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables.

Si l'incident de confidentialité présente un risque sérieux, la 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;
- 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;
- Aucun avis aux personnes visées n'est nécessaire si un tel avis aurait pour effet d'entraver une enquête faite par un Employé ou mandataire 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.

La 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

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

Par exemple, la Responsable pourrait demander :

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

6.5 Mesures à prendre s'il s'agit d'un incident de sécurité de l'information

La Responsable avise la Cheffe de la sécurité de l'information (CSIO) si l'incident constitue également un incident de sécurité de l'information, conformément au *Cadre de gestion de la sécurité de l'information*.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés au ministère de l'Éducation du Québec (MEQ) conformément à la *Directive gouvernementale sur la sécurité de l'information et du Processus de gestion des menaces, des vulnérabilités et des incidents* (GMVI) du Centre gouvernemental de cyberdéfense.

7 COMITÉ SUR L'ACCÈS

La Responsable peut en tout temps consulter le comité sur l'accès du CSSP dans l'analyse et le traitement d'une situation pouvant être un incident de confidentialité.

Elle transmet au Comité sur l'accès les recommandations de la Commission d'accès à l'information, le cas échéant.

8 INFORMATION ET DIFFUSION

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

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