Règles de gouvernance des renseignements personnels du CADRE

Fédération des établissements d'enseignement privés

Savoir réussir

Introduction

La confidentialité et la protection des renseignements personnels revêtent une importance primordiale pour La Fédération des établissements d'enseignement privés (FEEP), aussi connue sous le nom de Centre d'animation, de développement et de recherche en éducation (CADRE). Alors que les avancées technologiques transforment notre façon de collecter, de conserver et de traiter les données, il est essentiel d'établir des règles de gouvernance solides pour garantir la sécurité et la confidentialité des renseignements personnels. C'est dans cet objectif que le CADRE a élaboré le présent document sur les règles de gouvernance des renseignements personnels.

Ce document vise à fournir un cadre clair et rigoureux pour la gestion des renseignements personnels au sein du CADRE, notamment dans le cadre de ses activités. Il énonce des principes directeurs et des lignes directrices pratiques pour assurer la conformité légale, éthique et responsable dans le traitement des renseignements personnels.

Les règles de gouvernance des renseignements personnels énoncées dans ce document sont conçues pour répondre aux préoccupations croissantes en matière de confidentialité et de sécurité des données. Elles visent à protéger les droits fondamentaux des individus en matière de vie privée et encadrer la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements conformément à la Loi sur la protection des renseignements personnels dans le secteur privé.

En adoptant ces règles de gouvernance, le CADRE s'engage à préserver la confiance des individus qui participent à ses activités et à garantir la confidentialité et la sécurité de leurs renseignements personnels.

Dans les sections suivantes, nous présenterons les principes fondamentaux de la gouvernance des renseignements personnels établis par le CADRE. Ces principes serviront de guide pour tous ceux qui sont impliqués dans les activités du CADRE pour protéger la vie privée des individus et assurer une utilisation responsable des renseignements personnels.

Rôles et responsabilités des membres du personnel

RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Rôles

- Voir au respect de la protection des renseignements personnels au sein de l'établissement, mais aussi à l'égard de ceux confiés à un tiers;
- Promouvoir le droit au respect de la vie privée et de la protection des renseignements personnels au sein de l'établissement.

Responsabilités

Les responsabilités liées à la protection des renseignements personnels comprennent, mais ne se limitent pas, aux éléments suivants :

- Conseiller la direction en matière de protection des renseignements personnels.
- Siéger au Comité sur l'accès à l'information et sur la protection des renseignements personnels.
- Établir et mettre en œuvre les politiques et pratiques encadrant la gouvernance de l'établissement à l'égard des renseignements personnels et, veiller à sa révision périodique.
- Participer à l'établissement de la position organisationnelle en matière de protection des renseignements personnels.
- Intervenir à toute étape d'une évaluation des facteurs relatifs à la vie privée d'un projet visant un système d'exploitation ou de prestation électronique de services impliquant des renseignements personnels.
- Être consulté lors de l'évaluation du risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité.
- Tenir les registres de communications de renseignements personnels, incluant en cas d'incident de confidentialité.
- Être avisé en cas d'incident de confidentialité survenu chez un mandataire ou l'exécutant d'un contrat de service ou d'entreprise / Procéder (seul ou avec les services concernés) à l'inventaire des contrats avec des fournisseurs, prestataires externes et, le cas échéant, les réviser.
- Effectuer toute vérification relative à la confidentialité des renseignements personnels confiés à un tiers.
- Répondre aux demandes d'accès aux renseignements personnels, de rectification, aux plaintes.
- Prêter assistance au demandeur à comprendre la décision de lui refuser – en tout ou en partie – l'accès ou la rectification d'un renseignement personnel.
- Mettre en place des formations, des mécanismes de sensibilisation à la protection des renseignements personnels au sein de l'établissement.
- Répondre aux demandes de la Commission d'accès à l'information.

TECHNICIEN INFORMATIQUE

Rôles

- Voir au bon fonctionnement et à la conformité des systèmes, logiciels, licences et fournisseurs de services informatiques.
- Voir à la sécurité des systèmes informatiques, la gestion des accès conformément aux rôles des employés.
- Mettre en place les meilleures pratiques en matière de cybersécurité.

Responsabilités

Les responsabilités liées à la protection des renseignements personnels comprennent, mais ne se limitent pas, aux éléments suivants :

- Élaborer avec le Comité sur l'accès à l'information et la protection des renseignements personnels un plan d'intervention en cas d'incident de confidentialité.
- Établir les modalités des permissions d'accès et les gérer en collaboration avec les services concernés.
- Participer à la réalisation de l'inventaire des politiques, procédures, directives en lien avec la sécurité des renseignements personnels, le cas échéant les réviser ou en adopter de nouvelles;
- Dresser un inventaire des technologies utilisées pour collecter, communiquer et conserver les renseignements personnels.
- Participer à l'évaluation des facteurs relatifs à la vie privée en cas de refonte des sites et système informatiques.
- Établir les procédures quant à la destruction, l'anonymisation, la dépersonnalisation des renseignements personnels.
- S'assurer de la destruction des renseignements personnels détenus sur des supports informatiques conformément aux politiques de CADRE.
- Mettre en place des formations et des activités de sensibilisation quant à la sécurité des renseignements personnels et l'utilisation des ressources informatiques.
- S'assurer de la formation des nouveaux employés en matière de sécurité informatique.
- S'assurer du maintien de la formation continue en matière de sécurité informatique avec les employés et tenir le registre des formations à jour.

SECTEUR DES RESSOURCES FINANCIÈRES ET DES RESSOURCES HUMAINES

Rôles

- Recueillir les renseignements personnels dans le cadre de l'embauche du personnel et de la gestion de la paie, les adhésions aux avantages sociaux tels que le régime de retraite, les assurances collectives, la télémédecine, les programmes d'aide aux employés, le REER collectif ou tout autre intermédiaire de services relié aux conditions de travail de CADRE.
- Recueillir les renseignements personnels dans le cadre du paiement des fournisseurs et/ou consultants de CADRE.

Responsabilités du secteur des ressources financières et humaines

Les responsabilités liées à la protection des renseignements personnels comprennent, mais ne se limitent pas, aux éléments suivants :

- Dresser un inventaire des renseignements personnels détenus par chacun des services liés à la gestion financière et des ressources humaines, et ce, quels que soient le support et la répartition ou la circulation de ceux-ci.
- Dresser un inventaire de la documentation transmise aux employés quant à la collecte, l'utilisation, la communication et la conservation des renseignements personnels et, le cas échéant, la réviser à la lumière des exigences de la Loi 25.
- Déterminer et/ou revoir, de concert avec le secteur des ressources informatiques, les accès attribués à un employé, et ce, en fonction de son rôle au sein de son secteur.
- Mettre en œuvre les différentes politiques, procédures et directives déployées par CADRE quant à la collecte, l'utilisation, la communication, la conservation et la sécurité.
- S'assurer que les employés attestent annuellement avoir pris connaissance des différentes politiques et procédures applicables en matière de protection des renseignements personnels.
- Réviser les contrats avec les fournisseurs de services et organismes à qui des renseignements personnels sont transmis.

SECTEUR DU SERVICE DES ASSURANCES

Rôles

Recueillir et conserver des renseignements personnels nécessaires à la gestion des dossiers d'assurances. Les informations recueillies comportent, entre autres votre nom, prénom, adresse personnelle, adresse électronique, date de naissance, état matrimonial, sexe, numéro de téléphone, salaire, employeur, poste occupé, coordonnées bancaires et personnes à charge.

Responsabilités du secteur des assurances

Les responsabilités liées à la protection des renseignements personnels comprennent, mais ne se limitent pas, aux éléments suivants :

- Recueillir seulement les renseignements personnels nécessaires
- Recueillir les renseignements personnels dans des buts précis
- Faire tout en notre pouvoir, de concert avec le secteur des ressources informatiques, pour protéger les renseignements personnels, en limitant l'accès et à l'utilisation des renseignements personnels, et en protégeant nos installations et nos systèmes informatiques
- Conserver les renseignements personnels seulement le temps nécessaire pour :
    - Atteindre les buts pour lesquels nous les avons recueillis, et
    - Respecter nos obligations légales

PERSONNEL

(*S'applique également aux membres de la direction, aux employés surnuméraires, contractuels ou consultants)*

La protection des renseignements personnels est une responsabilité partagée au sein du Centre d'Animation, de Développement et de Recherche en Éducation (CADRE). Chaque membre du personnel a un rôle essentiel à jouer pour assurer la confidentialité et la sécurité des renseignements personnels et doit être conscient de l'importance de la confidentialité des renseignements personnels et de son impact sur les droits et la vie privée des individus.

Responsabilités

Les responsabilités liées à la protection des renseignements personnels comprennent, mais ne se limitent pas, aux éléments suivants :

- Se familiariser avec les politiques, les procédures et les pratiques du CADRE en matière de protection des renseignements personnels.
- Collecter uniquement les renseignements personnels nécessaires pour les finalités spécifiques reliées à l'exercice de leur fonction.
- Recueillir le consentement approprié des individus avant de collecter, utiliser ou divulguer des renseignements personnels, sauf si la loi le permet ou l'exige.
- Assurer la protection des renseignements personnels en utilisant les mesures de protection appropriées.
- Respecter les politiques et procédures de conservation des renseignements personnels selon le calendrier d'archivage.
- Accéder aux renseignements personnels uniquement lorsque cela est nécessaire à l'exécution d'une tâche ou d'une responsabilité professionnelle.
- Ne divulguer les renseignements personnels uniquement aux personnes autorisées et dans le respect des politiques et procédures du CADRE.
- Participer aux formations et aux séances d'information fournies par CADRE pour améliorer leur connaissance et compétences en matière de confidentialité et de protection des renseignements personnels.
- Attester sur une base annuelle avoir pris connaissance des différentes politiques et procédures applicables en matière de protection des renseignements personnels du CADRE et s'engager à les respecter.
- Signaler immédiatement tout incident de sécurité ou de violation présumée des renseignements personnels au Responsable de la protection des renseignements personnels.

Processus de traitement des plaintes relatives à la protection des renseignements personnels

Le CADRE reconnaît l'importance de traiter rapidement et efficacement les plaintes relatives à la protection des renseignements personnels. Nous nous engageons à résoudre les préoccupations des individus concernant la collecte, l'utilisation, la divulgation ou la sécurité de leurs renseignements personnels. Le processus de traitement des plaintes est le suivant :

1. Le dépôt de la plainte

Une personne peut déposer une plainte écrite en décrivant clairement les motifs et préoccupations concernant la protection des renseignements personnels. La plainte doit être adressée au Responsable de la protection personnel (RPRP).

2. Réception de la plainte et accusé de réception

Le RPRP reçoit la plainte et en accuse réception par courriel dans les 5 jours ouvrables de sa réception. Une copie de la plainte est conservée dans les dossiers à des fins de suivi et de référence ultérieure.

3. Évaluation de la plainte, enquête et résolution

Le RPRP examine la plainte de façon objective. Il peut faire appel au plaignant ou à d'autres parties pour comprendre les circonstances entourant l'incident. Si la plainte est jugée fondée, le RPRP met en place les mesures appropriées pour résoudre la situation, y compris la modification des politiques et pratiques.

4. Communication de la décision

Le RPRP communique par écrit la décision finale au plaignant en expliquant les conclusions de l'investigation et les actions prises pour résoudre la plainte ou la fermeture du dossier si elle n'est pas jugée fondée.

5. Suivi

Le RPRP consigne la plainte dans un registre et en fait rapport à la direction. Il met en place les ajustements nécessaires pour renforcer les pratiques en matière de protection des renseignements personnels du CADRE le cas échéant (si la plainte était fondée) Il assure un suivi des mesures correctives qui sont mises en œuvre.

Processus de traitement des demandes d'accès à l'information et modification

Le CADRE reconnaît l'importance de la transparence et de l'accès à l'information pour les individus. Conformément à la Loi sur la protection des renseignements dans le secteur privé, le processus pour traiter les demandes d'accès à l'information est les suivantes :

1. Le dépôt de la demande

Une personne peut déposer une demande d'accès à l'information écrite en décrivant clairement les documents ou les renseignements personnels auxquels ils souhaitent accéder ou faire modifier. La demande doit être adressée au Responsable de la protection personnel (RPRP).

2. Réception de la demande et accusé de réception

Le RPRP reçoit la demande et en accuse réception par courriel dans les 5 jours ouvrables de sa réception et informe le demandeur du délai de réponse de 30 jours pour donner suite à la demande.

3. Évaluation des documents

Le RPRP examine les documents collectés pour déterminer s'ils contiennent des informations qui doivent être protégées en vertu des exceptions prévues par la Loi. Si certaines informations sont considérées comme étant protégées, le RPRP peut procéder à une évaluation et à une consultation appropriée pour décider de la communication ou de la non-communication de ces informations.

4. Communication des documents

Le RPRP communique ou rectifie l'information dans un délai de 30 jours de la réception de la demande des documents. Si certains documents ne peuvent pas être communiqués en raison des exceptions prévues par la loi, le RPRP informe par écrit le demandeur des raisons de la non-communication et de ses droits de recours. L'absence de réponse dans ce délai équivaut un refus et donne droit 'exercer son droit de recours auprès de la Commission d'accès à l'information.

5. Suivi

Le RPRP consigne les demandes d'accès et la démarche effectuée pour repérer les documents dans un registre.

6. Recours

Le demandeur peut soumettre à la Commission d'accès à l'information une demande d'examen de mésentente relative à l'application d'une disposition législative portant sur l'accès ou la rectification d'un renseignement personnel comme prévu dans la Loi sur la protection des renseignements personnels dans le secteur privé.

Activités de formation et de sensibilisation

Le CADRE fait la promotion des meilleures pratiques et du respect des droits en matière de protection des renseignements personnels.

- Les employés reçoivent une formation afin de les sensibiliser à la protection des renseignements personnels et aux bonnes pratiques à mettre en œuvre dans la gestion des renseignements personnels et sur la cybersécurité.
- Les employés sont informés des procédures à suivre en cas d'incident de confidentialité, de plainte ou de demande d'accès à l'information ou modification.

Le Responsable de la protection des renseignements personnels fait le suivi des activités de formation dans un registre à cet effet.

Sondage

Le CADRE a établi les règles suivantes pour garantir la conformité et la protection des renseignements personnels lors de la réalisation de sondage.

Collecte de renseignements personnels

Lors de la réalisation de sondages, nous collectons uniquement les renseignements personnels nécessaires aux fins spécifiques du sondage.

Nous obtenons le consentement éclairé des participants avant de collecter leurs renseignements personnels, en expliquant clairement les objectifs du sondage et l'utilisation qui sera faite des données.

Utilisation des renseignements personnels

Les renseignements personnels collectés dans le cadre des sondages ne seront utilisés que dans le but spécifié au moment de la collecte. Nous ne partagerons pas les renseignements personnels avec des tiers sans le consentement explicite des participants, sauf si la loi l'exige ou le permet.

Protection des renseignements personnels

Nous mettons en place des mesures de sécurité appropriées pour protéger les renseignements personnels collectés dans le cadre des sondages contre tout accès non autorisé, la divulgation, l'altération ou la destruction. Nous veillons à ce que seules les personnes autorisées aient accès aux renseignements personnels et que celles-ci respectent strictement les politiques et procédures de protection des renseignements personnels du CADRE.

Conservation des renseignements personnels

Les renseignements personnels collectés dans le cadre des sondages seront conservés pendant la durée nécessaire pour atteindre les objectifs spécifiques du sondage, sauf si la loi exige ou permet une conservation plus longue. Une fois que les renseignements personnels ne sont plus nécessaires, nous les détruisons de manière sécurisée ou les rendons anonymes, conformément à la législation applicable.

Confidentialité et anonymat des participants

Nous veillons à préserver la confidentialité des participants en ne divulguant pas leurs réponses individuelles dans les rapports ou les résultats publiés. Lorsque cela est possible, nous encourageons l'anonymat des participants en évitant de collecter des renseignements personnels identifiables, sauf si cela est nécessaire pour atteindre les objectifs du sondage.

Conservation et destruction

Le CADRE assure la conservation et la destruction des renseignements personnels selon les normes d'archivage et le calendrier de conservation établie. La durée de conservation peut varier en fonction de la nature des renseignements, de la finalité de leur collecte et des exigences légales applicables.

Les renseignements personnels sont accessibles uniquement aux personnes autorisées qui ont besoin d'y accéder dans le cadre de leur fonction.

Les renseignements personnels confidentiels, tels que les renseignements sensibles, sont traités avec une attention particulière et des mesures de sécurité supplémentaires sont mises en place pour garantir leur protection.

Une fois que les renseignements personnels ne sont plus nécessaires ou que la période de conservation requise est terminée, nous les détruisons de manière sécurisée.

La destruction peut être effectuée par des méthodes telles que la destruction physique des documents papier ou l'effacement sécurisé des données électroniques, de manière que les renseignements ne puissent pas être récupérés ou reconstruits.

Plan d'action pour la gestion des incidents de confidentialité

Contexte

Le plan d'action pour la gestion des incidents de confidentialité s'inscrit dans le cadre des règles de gouvernance du CADRE.

1. Objectif

L'avènement d'un incident de confidentialité nécessite une action rapide afin que soient mises en place des mesures pour assurer la protection des renseignements personnels des personnes concernées et éviter que de nouveaux incidents de même nature se reproduisent.

Le présent plan d'intervention établit la procédure à suivre lorsqu'il y a motif de croire que s'est produit un incident de confidentialité. Il prévoit les rôles et responsabilités, les étapes de traitement, une grille d'évaluation du préjudice, des modèles d'avis ainsi qu'un registre des incidents de confidentialité.

2. Champ d'application

Le personnel et la direction de CADRE sont tenus de se conformer à ce plan d'intervention. La présente procédure s'applique également si un tiers détient des renseignements personnels pour le compte de CADRE.

3. Définitions

1) Incident de sécurité

Incident qui affecte la confidentialité, la disponibilité ou l'intégrité des informations d'un système ou la continuité de service de CADRE, incluant ou non des renseignements personnels.

2) Incident de confidentialité

Accès, utilisation et communication non autorisées par la loi d'un renseignement personnel, perte d'un tel renseignement ou toute autre atteinte à la protection de celui-ci.

3) Renseignements personnels

Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

4) Renseignement personnel sensible

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) Préjudice sérieux

Correspond à un acte ou à un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable.

4. Responsabilité

Le responsable de la protection des renseignements personnels est responsable de la mise en œuvre du Plan d'action au sein du CADRE.

5. Équipe de réponse en cas d'incident de sécurité et/ou de confidentialité

Rôle		Nom	Titre	Téléphone	Courriel
Interne	Responsable de la protection des renseignements personnels	Sylvain Filion	Directeur administration	514-381-8891 poste 250	filions@feep.qc.ca
	Responsable TI / sécurité	Martin Voghel	Technicien informatique	514-381-8891 poste 237	voghelm@feep.qc.ca
	Communication	Geneviève Beauvais	Directrice des communications	514-381-8891 poste 238	beauvaisg@feep.qc.ca
Externe	Service juridique	Me Cynthia Chassigneux de CHX Avocat			
	Assureur	BFL			
	Expert TI	Micro-Age			
	Commission d'accès à l'information			514 873-4196	cai.communications@cai.gouv.qc.ca

6. Étapes et démarches en cas d'incident de sécurité et/ou de confidentialité

- Toute personne qui a motif de croire que s'est produit un incident de confidentialité et /ou de sécurité doit aviser aussitôt son supérieur immédiat et le responsable de la protection des renseignements personnels.
- Le responsable de la protection des renseignements personnels avise le responsable TI et regroupe au besoin l'équipe de réponse.

* Les étapes suivantes peuvent être faites en simultané

6.1 Évaluer la situation

- Établir les circonstances de l'incident (heure, jour, lieu, personne qui a rapporté l'incident, etc.);
- Identifier les renseignements personnels impliqués;
- Identifier les personnes dont les renseignements personnels sont concernés;
- Trouver la cause (erreur humaine, vulnérabilité informatique, perte, vol, etc.).

Cette évaluation doit se poursuivre tant que tous les éléments n'ont pas été identifiés.

6.2 Diminuer les risques

Prendre rapidement les mesures raisonnables afin de diminuer les risques qu'un préjudice, qu'il soit sérieux ou non, ne soit causé et pour éviter que de nouveaux incidents de même nature ne surviennent, par exemple :

- Cesser la pratique non autorisée;
- Récupérer ou exiger la destruction des renseignements personnels impliqués;
- Corriger les lacunes informatiques;
- Inscrire une note dans les dossiers visés par un risque de vol d'identité;
- Exiger des vérifications supplémentaires;
- Révoquer ou modifier les mots de passe ou les codes d'accès informatiques.

6.3 Déterminer la nature du préjudice

Compléter la grille d'évaluation d'un incident de confidentialité (Annexe 1). Selon le résultat, la responsable de la protection des renseignements personnels détermine s'il y a absence ou présence d'un préjudice sérieux.

6.4 Absence de risque préjudice sérieux

- Inscrire l'incident au registre des incidents de confidentialité.

6.5 Présence d'un risque de préjudice sérieux

- Aviser dès que possible la Commission d'accès à l'information (CAI), même si l'ensemble des informations relatives à l'incident n'a pas encore été colligé (Formulaire).

- Aviser les personnes concernées par avis direct

- Pour agir plus rapidement pour diminuer le risque de préjudice, le CADRE pourrait transmettre un avis public si :
    - La transmission de l'avis direct peut causer un plus grand préjudice à la personne concernée;
    - La transmission de l'avis direct représente une difficulté excessive pour l'organisation;
    - L'organisation n'a pas les coordonnées de la personne concernée.

Un délai peut s'appliquer entre la connaissance de l'incident et l'avis aux personnes concernées. Ce délai peut être nécessaire pour compléter l'évaluation de la situation ou pour éviter d'entraver une enquête en cours par une personne ou un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

- Aviser toute autre personne ou organisme susceptibles de diminuer le risque
    - Service de police : si un crime semble avoir été commis.
    - L'assureur
    - Autres : il peut également être nécessaire d'aviser d'autres intervenants, tels que les agences de crédit, un mandataire, un cocontractant, une instance gouvernementale, un syndicat, un ordre professionnel, etc.
    - Le consentement de la personne concernée par l'incident de confidentialité n'est pas requis. Le cas échéant, il est recommandé d'inscrire cette communication au registre des incidents de confidentialité afin de conserver une trace documentaire de celle-ci (Destinataires, circonstances, renseignements transmis et objectifs de cette démarche).

6.6 Inscrire l'incident de confidentialité au registre

- Tous les incidents de confidentialité doivent être consignés au registre, même ceux qui ne présentent pas un risque de préjudice sérieux pour les personnes concernées;
- Le registre est complété par la responsable de la protection des renseignements personnels
- La durée de conservation est de cinq ans de la connaissance de l'incident de confidentialité.

6.7 Suivi et prévention

La responsable de la protection des renseignements personnels devra effectuer un post-mortem pour identifier et examiner les leçons tirées de l'incident, revoir les contrôles défaillants et réviser le plan d'action.