Annexes

Annexe 1 2

Processus de consentement exprès pour renseignements personnels sensibles 2

Consentement exprès pour renseignements personnels sensibles 4

Annexe 2 7

Processus de mise en œuvre du droit à la portabilité des renseignements personnels informatisés 7

Annexe 3 9

Processus – Confidentialité par défaut des produits et services technologiques 9

Annexe 4 11

Processus de conformité à l'article 65 – Information lors de la collecte de renseignements personnels 11

Annexe 5 13

Document explicatif – Demande d'informations - Conformité à la Loi 25 13

Annexe 6 15

Procédure de notification et de gestion des décisions fondées exclusivement sur un traitement automatisé de renseignements personnels 15

Annexe 7 18

Processus – Présentation des observations et révision humaine des décisions automatisées 18

Annexe 8 21

Procédure de contractualisation écrite des mandats confiés à des membres d'un ordre professionnel 21

Annexe 9 23

Modèle de clause contractuelle conforme à la Loi 25, à intégrer dans les mandats ou contrats confiés par un établissement à un membre d'un ordre professionnel 23

Annexe 10 25

Modèle d'analyse du régime juridique applicable hors Québec – Conformité à la Loi sur l'accès (article 70.1, Loi 25) 25

Annexe 11 27

Clause officielle pour les ententes, les appels d'offres, les contrats de service ou d'entreprise et les mandats 27

Annexe 12 28

Processus d'anonymisation et de dépersonnalisation 28

Annexe 13 31

Processus de gestion des demandes de portabilité des renseignements personnels 31

Annexe 14 33

Formulaire de consentement à la collecte, l'utilisation et la communication de renseignements personnels 33

Annexe 1

Processus de consentement exprès pour renseignements personnels sensibles

1. Objectif du processus

Assurer que toute nouvelle utilisation ou communication de renseignements personnels sensibles soit précédée d'un consentement manifesté de façon **expresse**, libre, éclairée et spécifique par la personne concernée.

2. Définition des renseignements personnels sensibles

- Sont considérés comme sensibles, notamment :
- Données médicales ou de santé
- Orientation sexuelle
- Opinions politiques ou religieuses
- Données biométriques
- Antécédents judiciaires
- Tout renseignement dont la divulgation peut porter atteinte à la personne concernée

3. Étapes du processus

a) Identification de la finalité

- Documenter la nouvelle finalité d'utilisation ou de communication.
- Vérifier que cette finalité est légitime, nécessaire et proportionnée.

b) Rédaction du formulaire de consentement exprès

Rédiger un formulaire distinct, clair et compréhensible.

Inclure :

- La nature des renseignements sensibles visés
- La finalité précise
- Les destinataires (internes ou externes)
- La durée de conservation
- Les droits de la personne (accès, rectification, retrait du consentement)

c) Obtention du consentement

- Présenter le formulaire à la personne concernée avant toute utilisation ou communication.
- S'assurer que le consentement est :
- Volontaire
- Spécifique à la finalité
- Documenté (signature ou validation électronique)

- Dans le cas des élèves mineurs, le consentement doit être obtenu auprès du titulaire de l'autorité parentale, sauf disposition contraire prévue par la Loi.

d) Enregistrement du consentement

- Conserver une copie du consentement dans un registre sécurisé.
- Associer chaque renseignement sensible à sa preuve de consentement.

e) Retrait du consentement

- Permettre à la personne de retirer son consentement à tout moment.
- Mettre en œuvre la suppression ou l'anonymisation des données concernées dans un délai raisonnable.

4. Responsabilités

Responsable de la protection des renseignements personnels (RPRP) :

- Supervise l'application du processus
- Valide les formulaires de consentement
- Répond aux demandes de retrait ou d'accès

Employés concernés :

- Formés sur les exigences du consentement exprès
- Tenus de respecter les étapes du processus

5. Contrôle et audit

- Vérification périodique de la conformité du processus
- Revue des consentements obtenus et des finalités associées
- Rapport annuel transmis à la direction

6. Références légales

- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1)
- Article 53 : Consentement requis
- Article 59 : Sensibilité des renseignements
- Article 65 : Retrait du consentement
- Loi 25 : Dispositions modifiant la Loi A-2.1 pour renforcer la gouvernance des renseignements personnels

Consentement exprès pour renseignements personnels sensibles

ARTICLE – X CONSENTEMENT EXPRÈS POUR L'UTILISATION ET LA COMMUNICATION DE RENSEIGNEMENTS PERSONNELS SENSIBLES

Toute nouvelle utilisation ou communication de renseignements personnels sensibles par [Nom de l'organisation] doit être précédée d'un **consentement manifesté de façon expresse** par la personne concernée.

À cet effet, l'organisation s'engage à :

1. **Définir clairement les renseignements personnels sensibles** visés, notamment ceux relatifs à la santé, à l'orientation sexuelle, aux croyances religieuses, aux données biométriques ou à toute autre information dont la nature exige une protection renforcée;
2. **Obtenir un consentement exprès**, distinct de tout autre document ou information, sous forme écrite ou électronique, selon les critères suivants :
    - Le consentement est **manifeste, libre, éclairé et spécifique**;
    - Il est **présenté dans un langage simple et compréhensible**;
    - Il précise la **finalité de l'utilisation ou de la communication**, les **tiers concernés**, et la **durée de conservation**;
3. **Conserver une preuve du consentement** dans un registre sécurisé, accessible uniquement aux personnes autorisées;
4. **Permettre à la personne concernée** de retirer son consentement à tout moment, et de demander la cessation de l'utilisation ou la suppression des renseignements concernés;
5. **Former le personnel** sur les exigences légales relatives au consentement exprès et sur les procédures internes à suivre;
6. **Réviser périodiquement les pratiques de consentement** afin d'assurer leur conformité aux exigences légales et aux meilleures pratiques en matière de protection des renseignements personnels.

Le non-respect de ces obligations peut entraîner des sanctions administratives ou pénales prévues par la Loi 25.

Formulaire de consentement exprès

1. Identification de l'organisation

Nom de l'organisation : _____

Adresse : _____

Personne responsable de la protection des renseignements personnels :

Nom : _____

Courriel : _____

Téléphone : _____

2. Renseignements personnels sensibles visés

Veuillez cocher les types de renseignements concernés :
☐ Informations relatives à la santé
☐ Orientation sexuelle
☐ Croyances religieuses ou philosophiques
☐ Données biométriques
☐ Autres (précisez) : _____

3. Finalité de l'utilisation ou de la communication

Les renseignements personnels sensibles seront utilisés ou communiqués aux fins suivantes :

_____

_____

4. Tiers concernés

Les renseignements pourront être communiqués aux tiers suivants :

_____

_____

5. Durée de conservation

Les renseignements seront conservés jusqu'au : _____

Ou selon la politique interne de conservation de l'organisation.

6. Consentement exprès

Je, soussigné(e),

Nom : _____

Date de naissance : _____

déclare avoir lu et compris les informations ci-dessus et **consens expressément** à

l'utilisation et à la communication de mes renseignements personnels sensibles selon les

modalités décrites.

☐ Je comprends que ce consentement est libre, éclairé, spécifique et distinct de tout autre document.
☐ Je comprends que je peux retirer mon consentement à tout moment en contactant la personne responsable mentionnée ci-dessus.
☐ Je comprends que je peux demander la suppression de mes renseignements personnels sensibles
☐ Je suis le parent ou le titulaire de l'autorité parentale de l'élève concerné (si applicable).

Signature : _____

Date : _____

Annexe 2

Processus de mise en œuvre du droit à la portabilité des renseignements personnels informatisés

Conformément à l'article 27 alinéa 3 de la Loi 25 (Québec)

1. Objectif

Assurer que tout projet impliquant la collecte de renseignements personnels informatisés permette à la personne concernée d'obtenir ses données dans un format technologique structuré et couramment utilisé, conformément à son droit à la portabilité.

2. Identification des données visées

- Déterminer les types de renseignements personnels informatisés recueillis directement auprès de la personne concernée.
- Exclure les données dérivées, inférées ou générées par l'organisation.

Exemples : Résultats scolaires, absences, plans d'intervention, formulaires médicaux, préférences pédagogiques.

3. Définition des formats de portabilité

- Sélectionner des formats technologiques **structurés et couramment utilisés**, tels que :
  - CSV (Comma-Separated Values)
  - JSON (JavaScript Object Notation)
  - XML (eXtensible Markup Language)
  - PDF (si structuré et lisible)
- Documenter les formats disponibles pour chaque type de donnée.

4. Intégration dans les systèmes d'information

- Développer ou adapter les systèmes pour permettre l'**exportation automatisée** des données dans les formats définis.
- Tester la compatibilité et l'interopérabilité des fichiers générés avec des outils tiers.
- Adapter les systèmes utilisés par l'école ou le centre de services scolaire (ex. Mozaïk, GPI) pour permettre l'exportation des données.

5. Mise en place d'un mécanisme de demande

- Créer une interface ou un formulaire permettant à la personne concernée de soumettre une demande de portabilité.
- Informer clairement sur :
  - Les types de données disponibles
  - Les formats proposés
  - Le délai de traitement (maximum 30 jours)

    - Les modalités de transmission sécurisée
- Vérifier l'identité du demandeur avant toute transmission.
- Dans le cas d'un élève mineur, la demande doit être faite par le titulaire de l'autorité parentale, sauf disposition contraire prévue par la Loi.

6. Transmission sécurisée des données

- Utiliser des moyens technologiques sécurisés pour transmettre les données :
    - Lien de téléchargement temporaire
    - Chiffrement des fichiers
    - Mot de passe ou authentification à double facteur

7. Suivi et traçabilité

- Tenir un registre des demandes de portabilité incluant :
    - Date de réception
    - Type de données transmises
    - Format utilisé
    - Mode de transmission
    - Identité du demandeur

8. Mesures organisationnelles complémentaires

- Intégrer le droit à la portabilité dans les politiques internes de protection des renseignements personnels.
- Former le personnel administratif, la direction, les secrétaires d'école et les équipes TI
- Réaliser une Évaluation des facteurs relatifs à la vie privée (ÉFVP) pour tout projet impliquant des données sensibles ou informatisées.

9. Références légales

- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1)
- Article 27 alinéa 3 – Droit à la portabilité
- Loi 25 – Dispositions modifiant la Loi A-2.1

10. Responsable

Le responsable de la protection des renseignements personnels est chargé de superviser la mise en œuvre de ce processus et de répondre aux demandes de portabilité.

Annexe 3

Processus – Confidentialité par défaut des produits et services technologiques

1. Objectif

Assurer que tout produit ou service technologique développé, acquis ou déployé par l'organisation soit configuré, dès sa mise en service, pour offrir **le plus haut niveau de confidentialité par défaut**, sans que la personne concernée ait à modifier les paramètres.

2. Champ d'application

Ce processus s'applique à :

- Sites web, applications mobiles, plateformes numériques
- Outils internes de gestion ou de communication
- Produits technologiques intégrant des fonctions de collecte, traitement ou communication de renseignements personnels
- Systèmes de gestion scolaire (ex. Mozaïk, GPI), plateformes pédagogiques, outils de communication avec les parents ou les élèves

3. Étapes du processus

a) Évaluation initiale

- Identifier les produits ou services technologiques concernés.
- Déterminer les types de renseignements personnels traités.
- Évaluer les paramètres de confidentialité existants.

b) Configuration par défaut

- Paramétrer chaque produit pour que :
  - La collecte de données soit **limitée au strict nécessaire**.
  - Les fonctions de partage, géolocalisation, profilage ou publicité soient **désactivées par défaut**.
  - L'accès aux données soit **restreint aux personnes autorisées**.
  - Les journaux d'activité soient **activés pour fins de traçabilité**.

c) Validation avant déploiement

- Intégrer une **vérification de conformité** dans le cycle de développement ou d'acquisition.
- Réaliser une **Évaluation des facteurs relatifs à la vie privée (ÉFVP)** pour tout nouveau produit ou service.
- Obtenir l'approbation du **Responsable de la protection des renseignements personnels (RPRP)**.

- Dans le contexte scolaire, cette validation peut être effectuée en collaboration avec le centre de services scolaire, notamment pour les outils partagés ou centralisés.

d) Documentation et traçabilité

- Documenter les paramètres de confidentialité appliqués.
- Conserver les preuves de configuration initiale et des mises à jour.
- Tenir un registre des produits et services conformes.

e) Surveillance continue

- Mettre en place un mécanisme de **vérification périodique** des paramètres.
- Assurer que les mises à jour logicielles ne modifient pas les niveaux de confidentialité par défaut.
- Prévoir une procédure de correction en cas de non-conformité.

4. Responsabilités

- **Développeurs et fournisseurs** : appliquer les paramètres requis dès la conception.
- **RPRP** : valider la conformité, superviser les ÉFVP, assurer la traçabilité.
- **Direction TI ou numérique** : intégrer le processus dans les pratiques d'acquisition et de développement.
- Dans une école secondaire, le **RPRP** est généralement le directeur ou une personne désignée par le centre de services scolaire.
- La **direction TI** peut être locale ou centralisée au niveau du centre de services scolaire selon le modèle organisationnel.

5. Références légales

- Article 9.1 – Loi 25 : « Les paramètres de confidentialité d'un produit ou d'un service technologique doivent être configurés de manière à offrir le plus haut niveau de confidentialité par défaut, sans intervention de la personne concernée. »
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1), modifiée par la Loi 25 (2021, chapitre 25), qui a apporté des changements à plusieurs lois, dont celle sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Annexe 4

Processus de conformité à l'article 65 – Information lors de la collecte de renseignements personnels

Conformément à la Loi sur l'accès et à la Loi 25 (Québec)

1. Objectif

S'assurer que tout nouveau procédé ou projet impliquant la collecte de renseignements personnels informe adéquatement la personne concernée, conformément aux exigences de l'article 65.

2. Identification des renseignements collectés

- Déterminer les types de renseignements personnels visés par le projet.
- Classer les données selon leur niveau de sensibilité (faible, moyen, élevé).
- Exemples : nom, adresse, résultats scolaires, absences, plans d'intervention, formulaires médicaux, coordonnées des parents.

3. Définition des finalités de la collecte

- Documenter clairement les objectifs de la collecte.
- Vérifier que chaque renseignement est **nécessaire et pertinent** pour la finalité déclarée.

4. Élaboration du contenu informatif à transmettre

Conformément à l'article 65, la personne concernée doit recevoir les informations suivantes **au moment de la collecte** :

- L'objectif de la collecte
- Les moyens par lesquels les renseignements sont recueillis
- Les droits d'accès et de rectification
- Le droit de retrait du consentement, s'il y a lieu
- Les catégories de personnes qui auront accès aux renseignements
- La durée de conservation
- Les mesures de sécurité mises en place
- Le nom et les coordonnées du responsable de la protection des renseignements personnels
- Dans le cas d'un élève mineur, l'information doit être communiquée au titulaire de l'autorité parentale, sauf disposition contraire prévue par la Loi.

5. Intégration dans les interfaces de collecte

- Ajouter un **avis de collecte clair et visible** dans :
  - Les formulaires papier ou numériques
  - Les interfaces web ou mobiles
  - Les communications verbales ou téléphoniques (si applicable)
  - o Les formulaires d'inscription scolaire ou de consentement parental
- S'assurer que l'information est :
  - Rédigée en langage simple
  - Accessible avant que la personne fournisse ses renseignements

6. Validation juridique et opérationnelle

- Faire valider le contenu informatif par le **responsable de la protection des renseignements personnels (RPRP)**.
- Réaliser une **Évaluation des facteurs relatifs à la vie privée (ÉFVP)** pour tout nouveau procédé.

7. Archivage et traçabilité

- Conserver une copie de l'avis de collecte utilisé pour chaque projet.
- Tenir un **registre des procédés de collecte** incluant :
  - Le type de données
  - Le canal de collecte
  - Le contenu informatif transmis
  - La date de mise en œuvre

8. Formation et sensibilisation

- Former les équipes impliquées dans la collecte (Direction, personnel administratif, enseignants, intervenants scolaires) sur :
  - Les obligations de l'article 65
  - Les bonnes pratiques de transparence
  - Les conséquences en cas de non-conformité

9. Responsable

Le **Responsable de la protection des renseignements personnels** est chargé de :

- Valider les avis de collecte
- Assurer la conformité des procédés
- Répondre aux demandes d'accès ou de rectification

Annexe 5

Document explicatif – Demande d’informations - Conformité à la Loi 25

1. Identification du dossier

- **Numéro de dossier** : *(à attribuer)*
- **Date de création du document** : *(ex. 25 août 2025)*
- **Personne responsable du traitement** : *(nom, titre)*

2. Description du cas

- **Type de situation** :
  ☐ Collecte de renseignements personnels
  ☐ Utilisation ou communication
  ☐ Incident de confidentialité
  ☐ Demande d’accès ou de rectification
  ☐ Traitement de données liées au dossier scolaire ou aux services aux élèves
  ☐ Autre : _____

- **Résumé du cas** :
  (Décrire clairement la situation, les personnes concernées, les données impliquées, et le contexte.)

3. Renseignements personnels concernés

- **Catégories de données** :
  ☐ Nom / Prénom
  ☐ Adresse courriel
  ☐ Numéro de téléphone
  ☐ Informations financières
  ☐ Données médicales
  ☐ Résultats scolaires
  ☐ Absences ou retards
  ☐ Plans d’intervention ou suivis psychosociaux
  ☐ Coordonnées des parents ou tuteurs
  ☐ Autres : _____

- **Sensibilité des données** :
  ☐ Faible
  ☐ Moyenne
  ☐ Élevée

4. Consentement et finalité

- **Consentement obtenu** : Oui / Non
  (Joindre preuve si disponible)
- **Finalité de la collecte ou de l'utilisation** :
  (Expliquer pourquoi ces données ont été recueillies ou utilisées.)

Note : Dans le cas d'un élève mineur, le consentement doit être obtenu auprès du titulaire de l'autorité parentale, sauf disposition contraire prévue par la Loi.

5. Mesures de sécurité

- **Mesures techniques et organisationnelles en place** :
  (Pare-feu, chiffrement, accès restreint, accès restreint aux dossiers scolaires, chiffrement des communications avec les parents via le portail Mozaïk etc.)
- **Évaluation des facteurs relatifs à la vie privée (ÉFVP)** :
  ☐ Réalisée
  ☐ Non requise
  ☐ En cours

6. Communication ou incident

- **Communication à des tiers** : Oui / Non
  (Préciser les destinataires et le cadre légal)
- **Incident de confidentialité** : Oui / Non
  (Si oui, décrire la nature de l'incident, les mesures prises, et joindre l'avis transmis à la CAI)

7. Réponse à la demande d'information

- **Demande reçue de** : *(Nom ou identifiant)*
- **Date de réception** :
- **Date de réponse** :
- **Documents transmis** :
  (Joindre copie ou résumé)

8. Suivi et archivage

- **Actions correctives ou préventives** :
  (Ex. mise à jour des politiques, formation du personnel, etc.)
- **Date de clôture du dossier** :
- **Archivage** :
  ☐ Physique
  ☐ Numérique
  ☐ Conforme aux exigences de conservation

Note : L'archivage doit respecter les règles de conservation établies par le centre de services scolaire et les exigences du ministère de l'Éducation.

Annexe 6

Procédure de notification et de gestion des décisions fondées exclusivement sur un traitement automatisé de renseignements personnels

1. Objectif

Assurer que toute personne concernée soit informée de manière transparente lorsqu'une décision la concernant est prise exclusivement par un traitement automatisé de ses renseignements personnels, conformément à l'article 12.1 de la Loi 25.

2. Portée

Cette procédure s'applique à tous les systèmes, processus ou outils utilisés par [Nom de l'organisation] qui prennent des décisions sans intervention humaine, incluant mais non limité à :

- Évaluation de candidatures
- Attribution de crédit ou tarification
- Profilage marketing
- Sélection ou exclusion automatisée

3. Définitions

- **Traitement automatisé** : Processus décisionnel effectué par un système informatique sans intervention humaine.
- **Personne concernée** : Toute personne dont les renseignements personnels sont utilisés dans le cadre du traitement automatisé.
- **Notification** : Communication formelle à la personne concernée concernant l'utilisation de ses données dans une décision automatisée.

4. Responsabilités

Rôle	Responsabilités
Responsable de la protection des renseignements personnels (RPRP)	Supervision de la procédure, validation des notifications
Responsable TI / IA	Documentation des systèmes automatisés, maintien du registre
Ressources humaines / Service client	Réception et traitement des demandes de révision humaine
Direction juridique	Appui à la conformité réglementaire

5. Étapes de la procédure

Étape 1 : Identification du traitement automatisé

- Recenser tous les processus décisionnels automatisés
- Documenter les finalités, les données utilisées et les impacts

Étape 2 : Information préalable

- Mettre à jour la politique de confidentialité
- Informer les personnes concernées **avant** la collecte ou l'utilisation des données

Étape 3 : Notification spécifique

- Lorsqu'une décision est prise, envoyer une notification contenant :
  - La nature du traitement automatisé
  - Les données utilisées
  - Les conséquences de la décision
  - Les droits de la personne (demande d'explication, contestation)

Étape 4 : Révision humaine

- Offrir un mécanisme clair pour demander une révision humaine :
  - Formulaire en ligne ou adresse courriel dédiée
  - Délai de réponse maximal : 30 jours
  - Révision effectuée par un agent qualifié

Étape 5 : Registre des décisions automatisées

- Tenir un registre contenant :
  - Date, type de décision, système utilisé
  - Données concernées
  - Notification envoyée
  - Résultat de la révision (le cas échéant)

6. Mesures de sécurité

- Accès restreint aux systèmes décisionnels
- Audit régulier des algorithmes
- Vérification de l'exactitude des données utilisées

7. Révision de la procédure

Cette procédure est révisée annuellement ou lors de toute modification législative ou technologique significative.

Annexe 7

Processus – Présentation des observations et révision humaine des décisions automatisées

1. Objectif

Garantir le droit de toute personne concernée de présenter ses observations à un membre du personnel compétent, lorsque la décision la concernant a été prise exclusivement par un traitement automatisé, et de demander une révision humaine de ladite décision.

2. Champ d'application

Ce processus s'applique à toute décision :

- Prise sans intervention humaine significative
- Ayant des conséquences juridiques ou importantes (ex. : refus de service, classification, exclusion)
- Rendue par un système automatisé ou algorithmique
- Attribution automatisée de cours ou de groupes
- Exclusion d'un programme ou d'une activité scolaire
- Traitement automatisé d'une demande de transport ou de service complémentaire
- Notification automatisée liée à l'assiduité ou au comportement

3. Étapes du processus

a) Notification initiale

- Informer la personne concernée qu'une décision a été prise exclusivement par un traitement automatisé
- Inclure dans la notification :
    - La nature de la décision
    - Les données utilisées
    - Les conséquences de la décision
    - Le droit de présenter des observations et de demander une révision humaine

b) Présentation des observations

- Offrir à la personne concernée les moyens suivants pour soumettre ses observations :
    - Formulaire en ligne sécurisé
    - Courriel dédié
    - Entretien téléphonique ou en personne (si applicable)
- Délai accordé : **15 jours ouvrables** suivant la notification

c) Réception et analyse

- Un **agent de révision désigné** reçoit les observations
- Analyse :
  - La décision initiale
  - Les données utilisées
  - Les observations formulées
- Peut demander des précisions ou des documents complémentaires

d) Révision humaine

- L'agent prend une décision révisée en tenant compte des observations
- Il peut :
  - Maintenir la décision
  - Modifier la décision
  - Annuler la décision

e) Communication de la décision révisée

- La personne reçoit une réponse écrite dans un délai de **30 jours ouvrables**
- La réponse inclut :
  - La décision révisée
  - Les motifs
  - Les recours possibles (le cas échéant)

4. Responsabilités

Rôle	Responsabilités
Responsable de la protection des renseignements personnels (RPRP)	Supervision du processus, validation des réponses (souvent le directeur ou une personne désignée par le centre de services scolaire)
Agent de révision désigné	Réception des observations, analyse de la décision, révision humaine (ex. direction pédagogique, conseiller d'orientation, intervenant scolaire)
Service des communications	Transmission des notifications et des formulaires (peut être le secrétariat ou le portail Mozaïk)
Direction	Appui à la mise en œuvre et à la formation du personnel

5. Registre et traçabilité

- Un registre est tenu pour chaque demande :
  - Identité de la personne
  - Type de décision
  - Observations reçues
  - Décision révisée
  - Délai de traitement

6. Références légales

- Article 12.1 – Loi 25 : Droit de la personne concernée de présenter ses observations à un membre du personnel en mesure de réviser la décision
- Guide d'application – Loi 25
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1), modifiée par la Loi 2

Annexe 8

Procédure de contractualisation écrite des mandats confiés à des membres d'un ordre professionnel

1. Objectif

Assurer que tout mandat confié par l'établissement à un professionnel membre d'un ordre soit formalisé par écrit, incluant les clauses de protection des renseignements personnels exigées par la Loi 25 et les clauses de protection des renseignements personnels exigées par la Loi 25 et conformément à la Loi sur les contrats des organismes publics (RLRQ, c. C-65.1).

2. Champ d'application

Cette procédure s'applique à tous les services professionnels externes impliquant le traitement de renseignements personnels (ex. : psychologues scolaires, orthophonistes, travailleurs sociaux, médecins-conseils, avocats spécialisés en droit de l'éducation).

3. Définitions

- **Mandat professionnel :** Entente entre l'établissement et un professionnel pour la prestation de services spécialisés.
- **Contrat écrit :** Document signé précisant les obligations, responsabilités et clauses de confidentialité.

4. Responsabilités

- **Direction de l'école:** Identifie le besoin de mandat et initie le processus.
- **RPRP :** Valide les clauses de protection des renseignements personnels.
- **Direction de l'école :** Approuve et signe le contrat.

5. Étapes du processus

Étape	Description	Responsable
1. Identification du besoin	Déterminer le type de service requis	Gestionnaire
2. Choix du professionnel	Sélectionner un membre d'un ordre reconnu	Gestionnaire
3. Rédaction du contrat	Utiliser le modèle standard incluant les clauses Loi 25, le modèle de contrat doit inclure les clauses de confidentialité exigées par la Loi 25 et respecter les directives du centre de services scolaire	Gestionnaire + RPRP
4. Validation juridique	Vérifier la conformité légale et réglementaire	RPRP
5. Signature	Obtenir les signatures officielles	Direction + Professionnel
6. Archivage	Conserver le contrat dans le registre des mandats	Secrétariat ou TI

6. Contrôles et suivi

- Audit annuel des mandats pour vérifier la présence de contrats écrits
- Rapport au comité de gouvernance de l'information
- Le rapport peut être transmis au comité de gouvernance du centre de services scolaire ou intégré au bilan annuel de conformité de l'établissement

7. Révision de la procédure

Cette procédure est révisée tous les 2 ans ou en cas de modification législative.

8. **Responsable :** Responsable de la protection des renseignements personnels (RPRP)

Annexe 9

Modèle de clause contractuelle conforme à la Loi 25, à intégrer dans les mandats ou contrats confiés par un établissement à un membre d'un ordre professionnel

Ce modèle vise à encadrer la protection des renseignements personnels dans le cadre de la prestation de services professionnels.

1. Objet de la clause

Le présent contrat encadre les obligations du professionnel en matière de protection des renseignements personnels, conformément à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1), telle que modifiée par la Loi 25

2. Définition des renseignements personnels

Aux fins du présent contrat, les « renseignements personnels » désignent toute information concernant une personne physique permettant de l'identifier, directement ou indirectement.

3. Obligations du professionnel

Le professionnel s'engage à :

- Traiter les renseignements personnels uniquement aux fins prévues au contrat.
- Mettre en place des mesures de sécurité raisonnables pour protéger les renseignements contre la perte, le vol, l'accès non autorisé, la divulgation ou la modification.
- Ne pas communiquer les renseignements à des tiers sans le consentement préalable de l'établissement ou de la personne concernée, sauf si requis par la loi.
- Informer immédiatement l'établissement de tout incident de confidentialité impliquant des renseignements personnels.
- Respecter les politiques internes de l'établissement ou du centre de services scolaire en matière de confidentialité et de gouvernance des renseignements personnels

4. Évaluation des facteurs relatifs à la vie privée (EFVP)

Lorsque le mandat implique un transfert de renseignements hors Québec ou un traitement automatisé, le professionnel collaborera à la réalisation d'une EFVP, conformément aux exigences de la Loi 25. Lorsque le mandat est encadré par le centre de services scolaire, la réalisation de l'EFVP peut être coordonnée avec celui-ci.

5. Droit d'accès et de rectification

Le professionnel reconnaît que les personnes concernées ont le droit d'accéder à leurs renseignements personnels et de les faire rectifier. Il s'engage à collaborer avec l'établissement pour répondre à ces demandes dans les délais prescrits.

6. Fin du contrat

À la fin du mandat, le professionnel devra :

- Retourner ou détruire les renseignements personnels selon les instructions de l'établissement.
- Certifier par écrit la destruction complète des données, le cas échéant.
- La destruction ou le retour des renseignements doit respecter les règles de conservation établies par le ministère de l'Éducation et le centre de services scolaire.

7. Surveillance et audit

L'établissement se réserve le droit de vérifier la conformité du professionnel aux obligations prévues par la Loi 25 ainsi qu'aux exigences légales applicables aux organismes publics, incluant, le cas échéant, celles de la Loi sur les contrats des organismes publics (RLRQ, c. C-65.1), notamment par des audits ou des demandes de documentation.

Les vérifications peuvent être effectuées par l'établissement ou par le centre de services scolaire, selon le niveau de contractualisation et les responsabilités partagées.

Annexe 10

Modèle d’analyse du régime juridique applicable hors Québec – Conformité à la Loi sur l’accès (article 70.1, Loi 25)

1. Identification du transfert

- **Type de transfert** :
  ☐ Communication à un fournisseur de services
  ☐ Hébergement de données à l’étranger
  ☐ Accès à distance par un tiers
  ☐ Utilisation d’une plateforme pédagogique ou d’un outil de gestion scolaire hébergé à l’extérieur du Québec
  ☐ Autre : _____

- **Pays ou territoire concerné** :
  (ex. États-Unis, France, Inde)
- **Destinataire des renseignements** :
  (Nom de l’organisation, rôle, lien contractuel)

2. Sensibilité des renseignements transférés

- Catégories de données :
  ☐ Identifiants personnels
  ☐ Données financières
  ☐ Données médicales
  ☐ Données biométriques
  ☐ Résultats scolaires
  ☐ Plans d’intervention
  ☐ Coordonnées des parents ou tuteurs
  ☐ Données liées à l’assiduité ou au comportement
  ☐ Autres : _____

- Niveau de sensibilité :
  ☐ Faible
  ☐ Moyenne
  ☐ Élevée

3. Finalité du transfert

- Objectif du transfert :
  (ex. traitement, stockage, analyse, support technique)
- Durée prévue du transfert ou de l’accès :
  (ex. temporaire, permanent, selon contrat)

4. Analyse du régime juridique étranger

- **Cadre légal applicable dans le pays de destination** :
  - Existe-t-il une loi sur la protection des renseignements personnels?
    ☐ Oui ☐ Non
  - Niveau de protection équivalent à celui du Québec?
    ☐ Oui ☐ Non
  - Principes reconnus :
    ☐ Consentement
    ☐ Droit d'accès et de rectification
    ☐ Limitation de la conservation
    ☐ Sécurité des données
    ☐ Supervision par une autorité indépendante
- **Risques identifiés** :
  (ex. surveillance étatique, accès non autorisé, absence de recours)

5. Mesures de protection mises en place

- **Mesures contractuelles** :
  - Contrat écrit avec clauses de confidentialité
  - Clauses spécifiques sur la protection des données
  - Engagement à ne pas sous-traiter sans autorisation
- **Mesures techniques** :
  - Chiffrement des données
  - Accès restreint
  - Journalisation des accès
- **Mesures organisationnelles** :
  - Formation du personnel
  - Politique interne de gestion des données
  - Audit régulier
  - Respect des politiques du centre de services scolaire en matière de gouvernance des renseignements personnels

6. Conclusion de l'analyse

- Le transfert est-il conforme à l'article 70.1 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, telle que modifiée par la Loi 25?
  ☐ Oui
  ☐ Non
  ☐ Conforme sous réserve de mesures supplémentaires
- Recommandations :
  (ex. renforcer les clauses contractuelles, limiter les données transférées, revoir la finalité)
- Date de l'analyse :
- Nom et fonction du responsable :
- *Signature :*

Annexe 11

Clause officielle pour les ententes, les appels d'offres, les contrats de service ou d'entreprise et les mandats

ARTICLE X – PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le Prestataire reconnaît que, dans le cadre de l'exécution du présent contrat, il pourrait avoir accès à des renseignements personnels au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1), telle que modifiée par la Loi 25.

À ce titre, le Prestataire s'engage à :

1. **Respecter l'ensemble des obligations légales** relatives à la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements personnels, conformément aux dispositions de la Loi 25 et conformément aux dispositions de la Loi 25 et aux politiques internes du centre de services scolaire ou de l'établissement.
2. **Utiliser les renseignements personnels uniquement aux fins prévues au contrat**, et s'abstenir de toute utilisation secondaire sans le consentement préalable et explicite du Client;
3. **Mettre en place des mesures de sécurité appropriées**, tant physiques, logiques qu'organisationnelles, afin de protéger les renseignements personnels contre tout accès, utilisation ou communication non autorisés;
4. **Informer sans délai le Client de tout incident de confidentialité**, incluant tout accès non autorisé, perte, vol ou compromission des renseignements personnels;
5. **Ne pas transférer les renseignements** personnels à l'extérieur du Québec sans avoir obtenu l'autorisation écrite préalable du Client et sans avoir réalisé une évaluation du régime juridique applicable dans le territoire de destination, conformément aux articles 17 et 70.1 de la Loi 25, et en collaboration avec le responsable de la protection des renseignements personnels de l'établissement ou du centre de services scolaire.
6. **Permettre au Client d'exercer ses droits** d'accès, de rectification, de retrait du consentement ou de suppression des renseignements personnels, et collaborer à toute demande en ce sens;
7. **Désigner une personne responsable** de la protection des renseignements personnels au sein de son organisation et transmettre ses coordonnées au Client, notamment pour faciliter les échanges avec le responsable désigné au sein de l'établissement scolaire.
8. **Collaborer à toute vérification ou audit** que le Client pourrait effectuer afin de s'assurer de la conformité aux obligations prévues par la Loi 25.

Le Prestataire reconnaît que toute violation des obligations prévues au présent article pourra constituer un manquement grave au contrat, pouvant entraîner sa résiliation immédiate sans préavis, et faire l'objet d'un signalement au comité de gouvernance du centre de services scolaire, le cas échéant.

Annexe 12

Processus d’anonymisation et de dépersonnalisation

1. Portée, objectif et utilisateurs

Le but de ce document est de fournir des conseils à l’**École secondaire de Bromptonville** (ci-après l’« **Établissement** ») pour établir et maintenir la dépersonnalisation et d’anonymisation de renseignements personnels.

Ces lignes directrices s’appliquent à tous les employés de l’Établissement, et particulièrement au responsable de l’accès à l’information et de la protection des renseignements personnels (« **Responsable RPRP** »), au responsable de la sécurité informatique, aux responsables des directions traitantes de Renseignements personnels, de même qu’au comité sur l’accès à l’information et la protection des renseignements personnels (le « **Comité** »).

2. Documents de référence

- *Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels*, c. A-2.1, telle que modifiée par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021 c 25 (la « **Loi sur l’accès** »);
- *Charte des droits et libertés de la personne,* RLRQ c C-12 (la « **CDLP** »)
- *Code civil du Québec*, RLRQ c CCQ-1991 (le « **CCQ** »).

3. Définitions

Les mots et expressions qui suivent, lorsqu’ils apparaissent avec une première lettre en majuscule aux présentes lignes directrices, ont le sens qui leur est attribué ci-dessous, à moins d’une dérogation implicite ou explicite dans le texte.

« Dépersonnalisation » signifie toute méthode, incluant la suppression des noms et identifiants évidents, permettant de faire en sorte qu'un renseignement personnel ne permette plus d'identifier directement la personne concernée.

« Anonymisation » désigne le traitement de renseignements personnels dans le but d’empêcher de *manière irréversible* l’identification de la personne à laquelle ils se rapportent. Les renseignements personnels peuvent être considérés comme anonymisés lorsqu’ils ne permettent pas d’identifier les personnes auxquelles ils se rapportent, et lorsqu’il n’est pas possible pour une personne d’être identifiée à partir des renseignements personnels par tout traitement ultérieur de ces mêmes données, ou en traitant ces mêmes données avec d’autres données disponibles ou susceptibles d’être disponibles. Pour la plupart des entreprises, l’anonymisation complète n’est pas possible.

4. Dépersonnalisation et Anonymisation de renseignements personnels

Les présentes lignes directrices répertorient une liste non exhaustive de techniques d'Anonymisation et de Dépersonnalisation pouvant être utilisées par l'Établissement. Elles sont fournies à titre indicatif uniquement et sujettes à être modifiées quant à l'anonymisation, advenant que le gouvernement adopte un règlement aux fins de déterminer les critères et les modalités applicables à l'anonymisation.

Lorsqu'on lui soumet une Activité de traitement nécessitant l'Anonymisation ou la Dépersonnalisation d'un Renseignement personnel, le Comité détermine les techniques appropriées d'Anonymisation et de Dépersonnalisation selon les Activités de traitement particulières de Renseignements personnels visés.

A. Anonymisation

En vertu de la Loi sur l'accès, lorsque les fins pour lesquelles un Renseignement personnel a été recueilli ou utilisé sont accomplies, l'Établissement doit le détruire ou l'anonymiser pour l'utiliser à des fins d'intérêt public, sous réserve de la Loi sur les archives (chapitre A-21.1).

Un Renseignement personnel anonymisé cesse d'être qualifié de Renseignement personnel et n'est plus soumis aux règles applicables en cette matière. Il pourra dès lors être utilisé, communiqué, diffusé et conservé sans autre obligation.

L'Établissement doit utiliser les mesures et les techniques généralement reconnues comme étant les meilleures pratiques en vue de faire l'Anonymisation de Renseignements personnels. En anonymisant un Renseignement personnel, l'Établissement doit tenir compte de la nature de ces renseignements, de leur quantité et des possibilités de faire des liens entre différents renseignements. Plusieurs techniques différentes peuvent être utilisées en combinaison.

Les méthodes suivantes seront utilisées par l'Établissement en tenant compte du degré de risque et de l'utilisation prévue des renseignements personnels.

1. **Remplacement de l'annuaire** – Modification du nom des personnes intégrées dans les listes de renseignements personnels, tout en maintenant la cohérence entre les valeurs, telles que « code postal + ville », « âge + sexe ».
2. **Brouillage** – Implique un mélange ou un obscurcissement des lettres. Le processus peut parfois être réversible. Par exemple : Robert pourrait devenir Betror.
3. **Masquage** – Permet de masquer une partie des renseignements personnels avec des caractères aléatoires ou d'autres données.
4. **Flou** – Approximation des valeurs des renseignements personnels pour rendre leur signification obsolète et/ou rendre impossible l'identification des individus.
5. **Confidentialité différentielle** – Cette méthode peut être utilisée chaque fois que l'Établissement donne à un tiers l'accès à un ensemble de données anonymisées. Une copie des renseignements personnels d'origine reste avec l'Établissement, et le destinataire tiers ne reçoit qu'un ensemble de données anonymes.
6. **Agrégation** – Une personne concernée est regroupée avec plusieurs autres personnes concernées qui partagent tout ou partie des renseignements personnels.

B. Dépersonnalisation

En vertu de la Loi sur l'accès, l'Établissement peut utiliser un Renseignement personnel sans le consentement de la Personne concernée lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé. Pour ce faire, l'Établissement doit prendre les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de Renseignements personnels dépersonnalisés.

Le Responsable AIPRP et le responsable des technologies de l'information établiront les méthodes de Dépersonnalisation appropriées telles que :

1. **Chiffrement (à l'aide d'une clé secrète)** – Les renseignements personnels sont chiffrés à l'aide d'une clé secrète. Le détenteur de la clé secrète peut réidentifier les personnes concernées en déchiffrant l'ensemble de renseignements personnels.
2. **Fonctions de hachage** – Utilisées pour mapper des renseignements personnels de n'importe quelle taille à des codes de taille fixe (notez qu'il existe plusieurs techniques de hachage (par exemple, salage, hachages à clé, etc.). Le salage est une méthode permettant de renforcer la sécurité des informations qui sont destinées à être hachées en y ajoutant une donnée supplémentaire afin d'empêcher que deux informations identiques conduisent à la même empreinte.
3. **Tokenisation** – Processus de substitution d'un élément de données sensibles par un équivalent non sensible, appelé jeton (Token). Le jeton est une référence (c'est-à-dire un identifiant) qui correspond aux données sensibles via un système de Tokenisation. Le système de Tokenisation fournit aux applications de traitement de données l'autorité et les interfaces nécessaires pour demander des jetons ou revenir à des données sensibles.

5. Mise à jour

La présente Politique est révisée, au besoin, suivant l'évolution du cadre normatif applicable en matière de protection des Renseignements personnels.

6. Entrée en vigueur

Ce document entre en vigueur à la date de son adoption par le Comité.

Annexe 13

Processus de gestion des demandes de portabilité des renseignements personnels

1. Objectif

Permettre à toute personne concernée d'exercer son droit à la portabilité en recevant ses renseignements personnels informatisés dans un format structuré et couramment utilisé, ou en les transférant à un tiers autorisé.

2. Champ d'application

Ce processus s'applique aux :

- Renseignements **informatisés**
- **Recueillis directement** auprès de la personne concernée
- **Non créés ou inférés** par l'organisation
- **Demandes explicites** de portabilité (distinctes du droit d'accès)
- **Données scolaires** ou administratives liées aux élèves, aux parents ou au personnel

3. Étapes du processus

a) Réception de la demande

- Moyens : formulaire web, courriel, courrier
- Vérification de l'identité du demandeur
- Enregistrement dans le registre des demandes

b) Validation de la portée

- Vérifier que les renseignements :
  - Sont informatisés
  - Ont été recueillis directement
  - Ne portent pas atteinte aux droits de tiers
- Refuser ou restreindre la demande si elle soulève des difficultés pratiques sérieuses

c) Préparation des données

- Extraire les données pertinentes
- Convertir dans un format **structuré et couramment utilisé** (ex. : JSON, CSV, XML)
- Vérifier l'intégrité et la lisibilité des données

d) Transmission

- Remettre les données :
  - À la personne concernée

    - Ou à un tiers autorisé, sur demande
- Mode sécurisé : téléchargement, courriel chiffré, portail sécurisé
- Dans le cas d'un élève mineur, la transmission peut être faite au titulaire de l'autorité parentale, sauf disposition contraire prévue par la Loi.

e) Confirmation et suivi

- Confirmer la transmission
- Documenter la demande, le traitement et la réponse
- Conserver les preuves de conformité

4. Rôles et responsabilités

Rôle	Responsabilités
Responsable de la protection des renseignements personnels (RPRP)	Supervision du processus, validation finale, réponse aux refus
Service des technologies de l'information (TI)	Extraction, formatage et transmission sécurisée des données
Service juridique	Analyse des risques, validation des tiers autorisés
Secrétariat de l'école ou le responsable désigné par le centre de services scolaire	Réception des demandes, communication avec le demandeur
Direction d'établissement ou celle du centre de services scolaire	Approbation des politiques, allocation des ressources

5. Délais recommandés

- Accusé de réception : **5 jours ouvrables**
- Traitement complet : **30 jours ouvrables**
- Prolongation possible en cas de complexité, avec avis au demandeur
- Ces délais sont conformes aux exigences de la Loi sur l'accès et peuvent être ajustés selon les directives du centre de services scolaire.

Annexe 14

Formulaire de consentement à la collecte, l'utilisation et la communication de renseignements personnels

1. Informations sur la personne concernée

- **Nom complet** : _____
- **Date de naissance** : _____/ _____ / _____
- **Téléphone** : _____
- **Courriel** : _____

2. Description des renseignements collectés

Veuillez cocher les types de renseignements que vous consentez à fournir :

☐ Coordonnées (adresse, téléphone, courriel)
☐ Informations d'identification (nom, date de naissance, numéro de dossier)
☐ Renseignements sensibles (voir section 3)
☐ Autres : _____

3. Consentement pour les renseignements sensibles

(Cochez uniquement si vous consentez à fournir ces renseignements)

☐ Renseignements de santé
☐ Origine ethnique ou culturelle
☐ Orientation sexuelle
☐ Opinions politiques ou religieuses
☐ Données biométriques (empreintes, reconnaissance faciale, etc.)

Ces renseignements sont collectés uniquement dans le cadre suivant :
Suivi psychosocial, services adaptés, intervention médicale, autres à spécifier

4. Consentement des mineurs de 14 ans et plus

☐ Je suis âgé(e) de 14 ans ou plus et je consens à la collecte, l'utilisation et la communication de mes renseignements personnels selon les modalités décrites ci-dessus.

☐ Je souhaite que mon parent ou tuteur légal soit informé de ce consentement.

Nom du parent/tuteur : _____

Téléphone :_____ Courriel : _____

Note : Conformément à la Loi sur l'accès, les mineurs de 14 ans et plus peuvent consentir seuls à la collecte de leurs renseignements personnels, sauf disposition contraire ou situation particulière.

5. Finalité de la collecte

Les renseignements sont recueillis pour les raisons suivantes :
☐ Fourniture de services
☐ Suivi administratif
☐ Analyse statistique
☐ Suivi pédagogique ou psychosocial
☐ Participation à des activités scolaires ou parascolaires
☐ Autres : _____

6. Durée de conservation

Les renseignements seront conservés pendant :
☐ Toute la durée de la relation avec l'organisme
☐ Une période de _____ années après la fin de la relation
☐ Selon la politique de conservation établie par le centre de services scolaire
☐ Autres : _____

7. Retrait du consentement

Vous pouvez retirer votre consentement en tout temps en contactant :

Par courriel : rprp@esb1954.com

Par Téléphone : 819-846-2738 poste 6302

Par courrier : Responsable de la protection des renseignements personnels
École secondaire de Bromptonville
125 rue du Frère-Théode
Sherbrooke QC
J1C 0S3

Note : Le retrait du consentement ne peut empêcher l'établissement de respecter ses obligations légales ou administratives.

8. Signature

Je déclare avoir lu et compris les informations ci-dessus et je consens à la collecte, l'utilisation et la communication de mes renseignements personnels.

Nom complet : _____

Date: _____/ _____ / _____

Signature : _____

(Si le requérant est mineur)

Nom complet du parent ou tuteur légal : _____

Date: _____/ _____ / _____

Signature : _____