

POLITIQUE DE GOUVERNANCE
À L'ÉGARD DES
RENSEIGNEMENTS PERSONNELS

Version 1.00 adoptée par le Conseil d'administration le 3 avril 2024

TABLE DES MATIÈRES

1. PRÉAMBULE.....	4
2. DÉFINITIONS.....	4
3. CADRE JURIDIQUE	5
4. CHAMP D'APPLICATION	6
5. COLLECTE DES RENSEIGNEMENTS PERSONNELS	7
5.1. Renseignements personnels pouvant être collectés.....	7
5.2. Informations communiquées lors de la collecte de renseignements personnels.....	7
6. UTILISATION DES RENSEIGNEMENTS PERSONNELS.....	7
7. CONSENTEMENT	8
8. COMMUNICATION DES RENSEIGNEMENTS PERSONNELS	8
8.1. Communication avec le consentement de la personne concernée	8
8.2. Communication sans le consentement de la personne concernée.....	8
8.3. Communication à la personne concernée.....	9
9. CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS	9
10. PROTECTION DES RENSEIGNEMENTS PERSONNELS	10
11. DEMANDE D'ACCÈS OU DE RECTIFICATION À DES RENSEIGNEMENTS PERSONNELS.....	10
11.1. Demande d'accès à des renseignements personnels.....	10
11.2. Demande de rectification	11
12. GESTION DES INCIDENTS DE CONFIDENTIALITÉ.....	12
12.1. Définition	12
12.2. Traitement d'un incident de confidentialité.....	12
12.3. Registre des incidents de confidentialité	13
13. PROCESSUS DE TRAITEMENT DES PLAINTES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	14
13.1. Dépôt d'une plainte relative à la protection des renseignements personnels.....	14
13.2. Traitement de la plainte	14
14. RÔLES ET RESPONSABILITÉS.....	14
14.1. Membres du personnel et toute personne œuvrant au nom de la Fondation	14
14.2. Consultants externes et prestataires de services	15
14.3. Direction générale de la Fondation	16
15. SANCTIONS APPLICABLES EN CAS DE NON-RESPECT DE LA PRÉSENTE POLITIQUE	16
16. DIFFUSION ET MISE À JOUR DE LA POLITIQUE.....	17
17. RESPONSABLE DE L'APPLICATION	17
18. ENTRÉE EN VIGUEUR ET RÉVISION DE LA POLITIQUE	17

ANNEXE 1 — RÈGLES DE CONSERVATION ET DE DESTRUCTION DES DOSSIERS	18
1. OBJECTIF	18
2. DÉFINITIONS	18
3. EXAMINER ET FERMER LE DOSSIER OU LE FICHIER	18
4. CONSERVATION DES DOSSIERS ET FICHIERS FERMÉS	19
5. DESTRUCTION DES DOSSIERS OU DES FICHIERS	19

1. PRÉAMBULE

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, aussi nommée Loi 25, a actualisé l'encadrement applicable à la protection des renseignements personnels et apporté des modifications législatives importantes aux dispositions de la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après la « Loi ») à laquelle les organismes de bienfaisance au Québec sont assujettis. Ces modifications visent à offrir une protection accrue des renseignements personnels, à offrir de nouveaux droits pour les citoyennes et les citoyens et à assurer une gestion des renseignements personnels plus responsable et transparente.

La Fondation du Cégep de Saint-Hyacinthe (ci-après la « Fondation ») doit désormais adopter des règles de gouvernance en matière de protection des renseignements personnels. La présente *Politique de gouvernance à l'égard des renseignements personnels* (ci-après la « Politique ») définit les principes directeurs pour assurer la protection des renseignements personnels, les processus pour demander l'accès à son dossier personnel, demander une rectification, les mécanismes pour signaler un incident de confidentialité et les rôles et responsabilités du personnel de la Fondation. Ces principes directeurs guident la Fondation dans la collecte, l'utilisation, la conservation et la destruction des renseignements personnels qu'elle détient, et ce, afin d'assurer la protection de ces renseignements tout au long de leur cycle de vie.



2. DÉFINITIONS

Dans cette Politique, les expressions et les termes suivants signifient :

Actifs informationnels : Information numérique, document numérique ou analogique, système d'information, documentation, matériel informatique, technologie de l'information, installation ou ensemble de ces éléments, acquis ou constitués par la Fondation pour mener à bien sa mission, qu'ils soient détenus ou exploités par la Fondation, par des prestataires de services ou par des tiers.

Collecte : Première étape du cycle de vie du renseignement personnel, la collecte est le moment où le renseignement personnel est recueilli, créé ou inféré, c'est-à-dire déduit à partir d'autres renseignements. Le fait de visualiser un renseignement personnel, comme ceux contenus sur une pièce d'identité, constitue également une collecte, même s'il n'y a pas de conservation par la suite.

Communication : Un renseignement personnel est communiqué dès qu'il est transmis à l'intérieur ou à l'extérieur de la Fondation, y compris à une entité externe associée à la Fondation.

Consentement : Autorisation de la personne titulaire des renseignements personnels à recueillir, utiliser et communiquer ses renseignements personnels. Le consentement ne se présume pas. Il doit être manifeste, libre, éclairé, être donné à des fins spécifiques, en termes simples et clairs, pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.

Conservation : conservation des renseignements personnels et ensemble de mesures adoptées pour les protéger.

Évaluation des facteurs relatifs à la vie privée : Démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques. Elle consiste à considérer les différents facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées.

Incident de confidentialité : Accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

Renseignements personnels : Tout renseignement se trouvant dans un document, peu importe sa forme et son support, qui concerne une personne physique et qui permet directement ou indirectement de l'identifier, tel que : nom, adresse, numéro de téléphone, adresse courriel, occupation, date de naissance, numéro d'assurance sociale, carte d'identité, scolarité, formation, diplôme, allergies ou restrictions alimentaires, photographies, renseignements bancaires, données de carte de crédit ou de débit, ou tout autre renseignement personnel nécessaire aux activités de la Fondation et à l'exercice de ses attributions (liste non exhaustive).

Système d'information : Système constitué des technologies de l'information, des procédures ainsi que des données qui y sont traitées, et dont le but est de fournir de l'information.

Utilisation : Tout usage, consultation ou accès à un renseignement personnel par les membres du personnel de la Fondation, incluant sa transmission entre ceux-ci ou entre ses différentes unités. Il ne s'agit pas d'une utilisation si le renseignement est transmis à une entité externe, mais d'une communication.

3. CADRE JURIDIQUE

La présente Politique est soumise, notamment, aux dispositions de :

- La *Loi sur la protection des renseignements personnels dans le secteur privé* (chapitre P-39.1) ;
- Le *Code civil du Québec* ;
- La *Charte des droits et libertés de la personne* ;

En cas de divergence entre la Loi et la présente Politique, la Loi prévaut.

4. CHAMP D'APPLICATION

La présente Politique s'applique à :

- Tout administrateur, tout membre du personnel de la Fondation et toute autre personne œuvrant au nom de la Fondation qui collecte, consulte, utilise, communique, détient ou conserve des renseignements personnels détenus par la Fondation et concernant toute personne physique indépendamment de l'endroit où ils sont utilisés ;
- Toute personne qui confie des renseignements personnels à la Fondation ;
- Tous les actifs informationnels de la Fondation contenant des renseignements personnels, durant tout leur cycle de vie, qu'ils soient conservés par la Fondation ou par un consultant externe ou un prestataire de service ;
- Tout consultant externe, prestataire de service ou autre tiers qui collecte, consulte, utilise, communique, détient ou conserve pour le compte de la Fondation des renseignements personnels.



5. COLLECTE DES RENSEIGNEMENTS PERSONNELS

5.1. Renseignements personnels pouvant être collectés

La Fondation peut recueillir des renseignements personnels afin de remplir adéquatement sa mission et d'assurer la bonne gestion de ses relations et de ses services avec chaque personne concernée. Cette collecte est limitée uniquement aux renseignements personnels nécessaires à l'objet du dossier. La Fondation prend des mesures pour s'assurer que les renseignements personnels qu'elle recueille sont adéquats, pertinents, non excessifs et utilisés aux seules fins pour lesquels ils ont été recueillis. Le consentement de la personne concernée est également nécessaire pour pouvoir légalement utiliser les renseignements personnels qu'elle transmet à la Fondation.

5.2. Informations communiquées lors de la collecte de renseignements personnels

Lorsqu'elle collecte des renseignements personnels afin de constituer un dossier sur quelqu'un, la Fondation s'assure d'informer la personne concernée, au plus tard au moment de la collecte :

- de l'objet du dossier ;
- de l'utilisation qui sera faite des renseignements ainsi que de personnes qui y auront accès au sein de la Fondation ;
- de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification. Sur demande, la personne concernée est également informée des renseignements personnels recueillis auprès d'elle, de la durée de conservation de ces renseignements ainsi que des coordonnées de la personne responsable de la protection des renseignements personnels.

6. UTILISATION DES RENSEIGNEMENTS PERSONNELS

La Fondation utilise des renseignements personnels concernant les étudiants et les membres du personnel du Cégep de Saint-Hyacinthe, ses donateurs et d'autres tierces parties, et ce, afin de s'acquitter de sa mission et de ses fonctions. Elle ne fait pas usage des renseignements personnels à d'autres fins que celles précisées lors de la collecte, à moins d'obtenir le consentement exprès de la personne concernée ou que la Loi sur la protection des renseignements personnels le permette. La Fondation s'assure ainsi de :

- Limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour les recevoir et lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions ;
- Limiter l'utilisation des renseignements personnels : à moins d'une exception prévue par la loi, elle doit obtenir le consentement de la personne concernée pour utiliser ses renseignements quand les fins pour lesquelles ceux-ci ont été collectés sont terminées ;
- Mettre en place des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits.

7. CONSENTEMENT

Dans les situations qui le requièrent, la Fondation doit transmettre un formulaire de consentement à la collecte, à l'utilisation ou à la communication des renseignements personnels aux personnes concernées. Pour être valable, le consentement doit être manifeste, libre, éclairé, donné à des fins spécifiques, en termes simples et clairs. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

Lorsqu'une personne a donné son consentement à la collecte, à l'utilisation ou à la communication de ses renseignements personnels, elle peut le retirer à tout moment. Pour retirer son consentement, elle peut communiquer avec la personne dont le nom est indiqué dans le formulaire de consentement. Dans le cas d'un refus de consentement ou d'un retrait, si la Fondation n'est pas en mesure de fournir un service particulier, elle explique l'impact du refus ou du retrait du consentement à la personne pour l'aider dans sa prise de décision.

8. COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

8.1. Communication avec le consentement de la personne concernée

La Fondation peut communiquer les renseignements personnels qu'elle détient ou certains d'entre eux si elle a obtenu préalablement le consentement valable de la personne concernée.

8.2. Communication sans le consentement de la personne concernée

La Fondation peut communiquer certains renseignements personnels détenus pour se conformer à l'ordonnance d'un tribunal, à une loi ou à une procédure judiciaire, y compris pour répondre à toute demande gouvernementale ou réglementaire, conformément aux lois applicables, ou encore, si la communication est nécessaire ou appropriée pour protéger les droits, la propriété ou la sécurité de la Fondation ou d'autres personnes.

La Fondation peut communiquer certains renseignements personnels qu'elle détient à un membre du personnel de la Fondation qui a la qualité pour le recevoir, c'est-à-dire lorsque ce renseignement est nécessaire à l'exercice de ses fonctions.

La Fondation peut communiquer les renseignements personnels qu'elle collecte à des consultants externes, des prestataires de services et à d'autres tiers qui la soutiennent. Ces consultants externes, des prestataires de services et autres tiers sont contractuellement obligés de garder les renseignements personnels confidentiels, de les utiliser uniquement aux fins pour lesquelles la Fondation les communique et de traiter les renseignements personnels selon les normes énoncées dans la présente Politique et en respect des lois.

La Fondation peut communiquer certains renseignements personnels à des fins d'étude, de recherche ou de production de statistiques sous réserve des conditions prévues par la Loi.

La Loi prévoit d'autres situations où la Fondation peut communiquer des renseignements personnels sans le consentement de la personne concernée.

8.3. Communication à la personne concernée

Les renseignements personnels que la Fondation détient sur une personne doivent lui être transmis sur demande de sa part.

En outre, la Loi prévoit le droit à la portabilité des renseignements personnels. Si la personne concernée le demande, la Fondation a l'obligation de lui communiquer, dans un format technologique structuré et couramment utilisé, un renseignement personnel informatisé recueilli auprès d'elle. Cette communication pourra aussi se faire à une personne ou à un organisme autorisé à recueillir le renseignement, à la demande de la personne concernée.

9. CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

La Loi exige que la Fondation mette en place des règles applicables à la conservation et à la destruction des renseignements personnels.

La Fondation documente où se retrouvent les dossiers matériels, papiers et informatiques contenant des renseignements personnels et limite l'accès à ces dossiers aux seules personnes ayant besoin de disposer de ses renseignements.

La Fondation ne conserve les renseignements personnels qu'elle détient que pour le temps nécessaire pour atteindre les fins pour lesquelles elle les a collectés, à moins que les exigences de la loi ou de la réglementation applicable prévoient un délai plus long. Lorsque la Fondation procède à la destruction de documents contenant des renseignements personnels, elle s'assure de prendre les mesures de protection nécessaires visant à assurer la confidentialité de ceux-ci. La méthode de destruction utilisée doit être déterminée en fonction de la sensibilité des renseignements, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support (voir l'Annexe 1).

Les renseignements personnels détenus par la Fondation sont traités et stockés au Québec. Dans l'éventualité où un transfert de renseignements personnels à l'extérieur du Québec est nécessaire dans le cadre de l'exercice des fonctions de la Fondation, ce transfert n'a lieu que s'il est évalué que le renseignement bénéficierait d'une protection adéquate, notamment en considérant la sensibilité du renseignement, la finalité de son utilisation, les mesures de protection dont le renseignement bénéficierait et le régime juridique applicable dans l'État ou la province où ce renseignement serait communiqué. Le transfert sera également soumis aux ententes contractuelles appropriées afin d'assurer cette protection adéquate.

Tout organisme doit définir la durée nécessaire du consentement obtenu de ses donateurs et des intervenants selon la fin pour laquelle les renseignements personnels ont été obtenus. La Fondation conserve les renseignements personnels obtenus de ses donateurs pour une durée maximale de 10 ans suivant la date de leur dernier don ou leur dernier consentement à l'utilisation de ses renseignements personnels, la date la plus récente ayant préséance. Ce consentement peut être renouvelé par les donateurs et les intervenants dans le cadre des liens et transactions effectuées avec la Fondation.

Les personnes pour lesquelles la Fondation détient des renseignements personnels peuvent demander en tout temps que leurs renseignements personnels soient détruits, désindexés ou anonymisés (à l'exception des informations requises figurant aux reçus pour fins de l'impôt sur le revenu pour une période de 6 ans).

10. PROTECTION DES RENSEIGNEMENTS PERSONNELS

La Fondation met en place des mesures de sécurité physiques, organisationnelles, contractuelles et technologiques appropriées et adéquates afin de protéger les renseignements personnels contre l'accès, la communication, la copie, l'utilisation ou la modification non autorisés par la loi, ainsi que la perte ou le vol. La Fondation prend des mesures pour faire en sorte que seuls les membres du personnel pour lesquels l'accès aux renseignements personnels dans le cadre de leurs fonctions est nécessaire soient autorisés à y accéder.

11. DEMANDE D'ACCÈS OU DE RECTIFICATION À DES RENSEIGNEMENTS PERSONNELS

11.1. Demande d'accès à des renseignements personnels

Toute personne qui en fait la demande a le droit d'accès aux renseignements personnels la concernant détenus par la Fondation, sous réserve des exceptions prévues par la Loi.

Une demande d'accès ne peut être considérée que si elle est faite par écrit par une personne physique justifiant de son identité à titre de personne concernée, à titre de représentante ou de représentant, d'héritière ou d'héritier ou de successible de cette dernière, à titre de liquidatrice ou de liquidateur de la succession, à titre de bénéficiaire d'assurance vie ou d'indemnité de décès, à titre de titulaire de l'autorité parentale même si l'enfant mineur est décédé, ou à titre de conjointe ou de conjoint ou de proche parent d'une personne décédée.

Cette demande doit être adressée à la personne responsable de la protection des renseignements personnels de la Fondation qui peut être jointe à l'adresse courriel suivante : fondation@cegepsth.qc.ca. La demande doit fournir suffisamment d'indications précises pour permettre à la Fondation de la traiter. La personne responsable doit répondre au plus tard dans les trente (30) jours suivant la date de la réception d'une demande. Si la personne qui fait la demande n'est pas satisfaite de la réponse de la Fondation, elle peut déposer une demande d'examen de mécontentement auprès de la Commission d'accès à l'information. Cette demande doit être faite dans les trente (30) jours qui suivent la date de la décision ou de l'expiration du délai prévu à la Loi.

11.2. Demande de rectification

Toute personne qui reçoit une confirmation de l'existence dans un fichier d'un renseignement personnel la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la Loi, exiger que le fichier soit rectifié. Une demande de rectification ne peut être considérée que si elle est faite par écrit par une personne physique justifiant de son identité à titre de personne concernée, à titre de représentante ou de représentant, d'héritière ou d'héritier ou de successible de cette dernière, à titre de liquidatrice ou de liquidateur de la succession, à titre de bénéficiaire d'assurance vie ou d'indemnité de décès, à titre de titulaire de l'autorité parentale même si l'enfant mineur est décédé ou à titre de conjointe ou de conjoint ou de proche parent d'une personne décédée.

Cette demande doit être transmise à la personne responsable de la protection des renseignements personnels de la Fondation qui peut être jointe à l'adresse courriel suivante : fondation@cegepsth.qc.ca. La demande doit fournir suffisamment d'indications précises pour permettre à la Fondation de la traiter. La personne responsable doit répondre au plus tard dans les trente (30) jours suivant la date de la réception d'une demande.

La Fondation doit, lorsqu'elle accède à une demande de rectification d'un fichier, délivrer sans frais à la personne qui l'a demandé une copie de tout renseignement personnel modifié ou ajouté, ou, selon le cas, une attestation du retrait d'un renseignement personnel. Lorsque la Fondation refuse en tout ou en partie d'accéder à une demande de rectification d'un fichier, la personne concernée peut exiger que cette demande soit enregistrée. Si la personne qui fait la demande n'est pas satisfaite de la réponse de la Fondation, elle peut déposer une demande d'examen de mécontentement auprès de la Commission d'accès à l'information. Cette demande d'examen de mécontentement doit être faite dans les trente (30) jours qui suivent la date de la décision ou de l'expiration du délai prévu à la Loi.

12. GESTION DES INCIDENTS DE CONFIDENTIALITÉ

12.1. Définition

Au sens de la présente Politique, constitue un incident de confidentialité :

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

Pour fins de clarification, sont considérés comme des incidents de confidentialité les exemples suivants :

- Consulter des renseignements personnels non nécessaires à l'exercice de ses fonctions ;
- Outrepasser les droits d'accès qui ont été consentis à une personne pour consulter un renseignement personnel ;
- Utiliser des renseignements personnels d'une base de données à laquelle une personne a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne ou d'altérer des renseignements ;
- Communiquer un renseignement personnel par erreur à la mauvaise personne ;
- La perte ou le vol de documents contenant des renseignements personnels ;
- Oublier de caviarder des renseignements personnels dans un document destiné à une personne n'ayant pas la qualité de les recevoir ;
- Partager sans autorisation de renseignements personnels à son équipe ou à son groupe alors que certains membres n'ont pas la qualité pour recevoir ces informations ;
- Être victime d'une cyberattaque, tels de l'hameçonnage ou un rançongiciel.

12.2. Traitement d'un incident de confidentialité

Lorsque la Fondation a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient, elle doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent. La Fondation avise sans délai la personne responsable de la protection des renseignements personnels.

La Fondation peut également aviser toute personne ou tout organisme susceptibles de diminuer ce risque en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée. Dans ce dernier cas, la personne responsable de la protection des renseignements personnels doit consigner la communication. Si l'incident de confidentialité présente un risque qu'un préjudice sérieux soit causé, la Fondation doit, avec diligence, aviser toute personne dont un renseignement personnel est concerné par l'incident. Elle doit également aviser la Commission d'accès à l'information. Afin d'évaluer le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, la Fondation doit considérer, notamment :

- La sensibilité du renseignement concerné ;
- Les conséquences appréhendées de son utilisation ;
- La probabilité qu'il soit utilisé à des fins préjudiciables.

12.3. Registre des incidents de confidentialité

La Fondation tient un registre des incidents de confidentialité. Celui-ci contient, notamment :

- Une description des renseignements personnels visés par l'incident ;
- Les circonstances de l'incident ;
- La date où l'incident a eu lieu ;
- La date où la personne responsable de la protection des renseignements personnels a eu connaissance de l'incident ;
- Le nombre de personnes visées ou, s'il n'est pas connu, une approximation de ce nombre ;
- L'évaluation de la gravité du risque de préjudice ;
- S'il existe un risque de préjudice sérieux pour la personne concernée, les dates de transmission des avis ;
- Les mesures prises en réaction à l'incident.

Les informations contenues au registre doivent être tenues à jour et conservées pendant une période minimale de cinq ans après la date ou la période au cours de laquelle la Fondation a pris connaissance de l'incident.

13. PROCESSUS DE TRAITEMENT DES PLAINTES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

13.1. Dépôt d'une plainte relative à la protection des renseignements personnels

Tout membre du personnel de la Fondation et toute personne ayant confié des renseignements personnels à la Fondation qui a des motifs de croire qu'un incident de confidentialité s'est produit et que la Fondation a fait défaut de protéger la confidentialité des renseignements personnels qu'elle détient peut déposer une plainte pour demander que la situation soit corrigée. La plainte doit être déposée par écrit. Elle doit comporter une description de l'incident, la date ou la période où l'incident s'est produit, la nature des renseignements personnels visés par l'incident et le nombre de personnes concernées. La plainte doit être transmise à la personne responsable de la protection des renseignements personnels. Dans le cas où la plainte mettrait en cause la conduite de la personne responsable de la protection des renseignements personnels, celle-ci doit être transmise au conseil d'administration de la Fondation.

13.2. Traitement de la plainte

La personne responsable de la protection des renseignements personnels ou la direction générale de la Fondation, le cas échéant, a la responsabilité de traiter la plainte dans un délai maximal de 30 jours ouvrables. Dans le cas où celle-ci s'avérait fondée, la Fondation prend les mesures requises pour corriger la situation dans les meilleurs délais, et ce, conformément au paragraphe 11.2 de la présente Politique. Elle procède à l'inscription de l'incident au registre, comme indiqué au paragraphe 12.3.

14. RÔLES ET RESPONSABILITÉS

14.1. Membres du personnel et toute personne œuvrant au nom de la Fondation

Les membres du personnel ont la responsabilité de :

- Respecter la présente Politique ;
- Participer aux activités de sensibilisation et de formation offertes par la Fondation ;
- Communiquer les informations requises au paragraphe 5.2 de la présente Politique lors de la collecte de renseignements personnels ;
- S'assurer d'avoir la qualité requise ou le consentement avant de collecter ou d'utiliser un renseignement personnel ;
- S'assurer lors de la communication d'un renseignement personnel que le destinataire a la qualité requise pour le recevoir ou qu'un consentement autorise cette communication ;
- Faire signer une entente de confidentialité avant de communiquer un renseignement personnel à un consultant externe ou un prestataire de services ;

- Faire des efforts raisonnables pour minimiser le risque de communication non intentionnelle de renseignements personnels ;
- Prendre les précautions nécessaires pour s'assurer que les renseignements personnels ne sont pas surveillés, entendus, consultés ou perdus lorsqu'ils travaillent dans des locaux autres que les bureaux de la Fondation ;
- Rapporter sans délai un incident de confidentialité au responsable de la protection des renseignements personnels de la Fondation ;
- Rapporter sans délai au responsable de la protection des renseignements personnels toute communication à un tiers faite sans le consentement de la personne concernée ;
- Ne conserver les renseignements personnels que pour le temps nécessaire pour atteindre les fins pour lesquelles ils ont été collectés, à moins que la Loi ou la réglementation prescrivent un délai de conservation plus long ;
- Collaborer dans la recherche de documents et d'informations faisant l'objet de toute demande d'accès ;
- S'assurer de prendre les mesures de protection nécessaires visant à assurer la confidentialité des renseignements personnels lors de leur destruction.

14.2. Consultants externes et prestataires de services

Les consultants externes et les prestataires de services ayant accès à des renseignements personnels que la Fondation détient ont la responsabilité de :

- Respecter la présente Politique ;
- Signer un engagement de confidentialité et faire signer un engagement de confidentialité à toute personne qui sera appelée à consulter les renseignements personnels dans le cadre de l'exécution du contrat ;
- Communiquer les informations requises au paragraphe 5.2 de la présente Politique lors de la collecte de renseignements personnels ;
- S'assurer d'avoir la qualité requise ou le consentement avant de collecter ou d'utiliser un renseignement personnel ;
- S'assurer lors de la communication d'un renseignement personnel que le destinataire a la qualité requise pour le recevoir ou qu'un consentement autorise cette communication ;
- Faire des efforts raisonnables pour minimiser le risque de communication non intentionnelle de renseignements personnels ;
- Prendre les précautions nécessaires pour s'assurer que les renseignements personnels ne sont pas surveillés, entendus, consultés ou perdus lorsqu'ils travaillent dans des locaux autres que les locaux de la Fondation ;
- Rapporter sans délai un incident de confidentialité à la Fondation ;

- Rapporter sans délai à la Fondation toute communication à un tiers faite sans le consentement de la personne concernée ;
- Conserver les renseignements personnels que pour le temps nécessaire pour l'exécution de leur contrat à moins que la Loi ou la réglementation applicable prescrivent un délai de conservation plus long ;
- S'assurer de prendre les mesures de protection nécessaires visant à assurer la confidentialité des renseignements personnels lors de leur destruction.

14.3. Direction générale de la Fondation

La direction générale a la responsabilité de :

- Agir à titre de personne responsable de la protection des renseignements personnels ;
- Appliquer la présente Politique et assurer son suivi et sa révision ;
- Veiller à faciliter le respect et la mise en œuvre de la présente Politique ;
- Mettre à la disposition des employés les ressources nécessaires à l'atteinte des objectifs de la Politique ;
- Maintenir à jour le registre des incidents de confidentialité ;
- Informer la Commission d'accès à l'information et la personne concernée de tout incident de confidentialité présentant un risque de préjudice sérieux ;
- Traiter les demandes d'accès à l'information ;
- Traiter les demandes de rectifications ;
- Planifier et assurer la réalisation des activités de formation ;
- Recevoir les plaintes relatives à la présente Politique, déterminer leur recevabilité et, le cas échéant, les transmettre à l'instance concernée ;
- S'assurer que les consultants externes et les prestataires de services signent une entente de confidentialité et prennent les mesures nécessaires à l'application et au respect de la Politique.

15. SANCTIONS APPLICABLES EN CAS DE NON-RESPECT DE LA PRÉSENTE POLITIQUE

Le non-respect de la présente Politique pourrait entraîner des mesures administratives ou disciplinaires pouvant aller jusqu'au congédiement. La nature, la gravité et le caractère répétitif des actes reprochés doivent être considérés au moment de déterminer une sanction.

Des sanctions sont également prévues dans la Loi en cas de manquement. Dans le cadre de ses relations contractuelles avec un tiers, la Fondation peut mettre fin à tout contrat sans préavis pour non-respect de la présente Politique. Celle-ci sera présentée à tous les tiers contractants avec la Fondation, lesquels devront s'engager, par écrit, à s'y conformer.

16. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

La direction générale de la Fondation s'assure de la diffusion et de la mise à jour de la Politique sur le site Web de la Fondation.

17. RESPONSABLE DE L'APPLICATION

La direction générale de la Fondation est responsable de l'application de la Politique et de sa révision.

18. ENTRÉE EN VIGUEUR ET RÉVISION DE LA POLITIQUE

La présente Politique est adoptée par le conseil d'administration et entre en vigueur le **JOUR MOIS ANNÉE**.

ANNEXE 1 — RÈGLES DE CONSERVATION ET DE DESTRUCTION DES DOSSIERS

1. OBJECTIF

L'objectif de ces règles est de fournir des procédures de fermeture, de conservation et de destruction des dossiers et des fichiers maintenus par la Fondation du Cégep de Saint-Hyacinthe (ci-après la « Fondation »).

2. DÉFINITIONS

Dans les présentes règles, les expressions et les termes suivants signifient :

Date de fermeture d'un dossier ou d'un fichier : date à laquelle le responsable détermine que le dossier ou le fichier est achevé et à partir de laquelle il détermine la destruction du dossier ou du fichier.

Date de destruction d'un dossier ou d'un fichier : date à partir de laquelle un dossier ou un fichier peut être détruit.

Dossier ou fichier : un document papier ou un dossier informatique pouvant contenir des renseignements personnels. Un fichier de donateur dans la base de données contenant généralement des renseignements personnels représente un fichier au regard des présentes règles.

3. EXAMINER ET FERMER LE DOSSIER OU LE FICHIER

Quand un dossier ou un fichier est achevé, le responsable détermine sa date de fermeture et sa date de destruction. Un dossier ou un fichier comportant des renseignements personnels peut être détruit, anonymisé ou désindexé selon la loi.

Quand un dossier ou un fichier est clos, la Fondation verse une note à cet effet dans ses registres. La Fondation tient des registres identifiant les dossiers et fichiers clos, y compris la date de fermeture et le cas échéant, la date de destruction.

Avant de fermer un dossier physique, le responsable doit prendre les mesures requises pour que tout renseignement personnel au dossier soit détruit, notamment par déchiquetage. La Fondation doit aussi supprimer des doubles de copies électroniques de documents qui ont été sauvegardés.

4. CONSERVATION DES DOSSIERS ET FICHIERS FERMÉS

Les dossiers fermés sont entreposés dans un lieu physique pour maintenir la confidentialité des renseignements personnels obtenus et pour les protéger contre les dommages ou la perte. Ils peuvent aussi être conservés sur un support informatique sous forme de fichier.

5. DESTRUCTION DES DOSSIERS OU DES FICHIERS

La Fondation détruira tout dossier ou fichier pour lesquels aucun consentement à l'utilisation des renseignements personnels n'a été obtenu au 22 septembre 2023 ou pour lesquels un consentement a été consenti il y a plus de dix (10) ans.

Quand le responsable ferme le dossier ou le fichier et si ce dernier est prêt pour la destruction, la date de destruction est déterminée selon la norme définie par la Fondation à moins que le responsable détermine qu'une autre date de destruction convient mieux.

La Fondation conserve les dossiers et les fichiers fermés principalement pour satisfaire aux craintes concernant la gestion du risque. En conséquence, le dossier ou le fichier fermé doit être conservé pendant une période déterminée selon la prescription durant laquelle des réclamations peuvent être déposées à l'égard de la Fondation. Dans le doute, le responsable doit désigner la période applicable la plus longue qui précède la date de destruction. La date de destruction pour la plupart des dossiers et fichiers doit être de dix (10) ans après la date de fermeture fixée par le responsable. Une autre date de destruction des dossiers et des fichiers peut être fixée par le responsable, selon les circonstances.

La date de destruction doit être suspendue dans les cas suivants se rapportant directement ou indirectement à :

- a) une réclamation réelle ou potentielle déposée contre la Fondation ;
- b) une demande de divulgation portant sur les renseignements personnels obtenus par la Fondation ;
- c) un audit ou une enquête gouvernementale, pouvant également être ordonné par la personne responsable de la protection des renseignements personnels.

La date de destruction des dossiers et fichiers peut également être reportée à tout moment, au besoin.

Ces règles s'appliquent de manière à assurer le maintien de la confidentialité des renseignements personnels contenus aux dossiers et aux fichiers et le respect des lois applicables en matière de protection des renseignements privés.

Toute fermeture ou destruction de dossier ou de fichier doit au préalable être autorisée par la personne responsable de la protection des renseignements personnels.