DIRECTIVES ET PROCÉDURES

DIRECTIVES ADMINISTRATIVES	DE NATURE GÉNÉRALE
TITRE :	**ACCÈS À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE**
CODE NUMÉRIQUE :	GEN-09
RESPONSABLE DE LA DIFFUSION :	Vice-présidence des Ressources humaines et culture organisationnelle
PERSONNES OU GROUPES CONSULTÉS :	
ENTRÉE EN VIGUEUR :	10 mai 2004
DERNIÈRE RÉVISION :	21 octobre 2020
FRÉQUENCE DE RÉVISION	Cette directive est révisée et validée à tous les 5 ans.

Dans le présent document, le genre masculin est utilisé afin d'alléger le texte et se veut inclusif et utilisé autant pour désigner les femmes, les hommes et le genre neutre.

1. OBJET

Le Collège La Cité entend respecter, dans toutes ses opérations, les objets et dispositions de la *Loi sur l'accès à l'information et la protection de la vie privée* (ci-après *LAIPVP*) ainsi que de tout autre texte législatif portant sur la protection de la vie privée susceptible d'avoir une incidence sur les opérations et activités du Collège. Le Collège veut ainsi s'assurer que :

a) la cueillette par le Collège de renseignements personnels soit faite en conformité avec le paragraphe 38 (2) de la *LAIPVP* soit que : *nul ne doit recueillir des renseignements personnels pour le compte d'une institution à moins d'y être autorisé expressément par une loi, ou à moins que ces renseignements servent à l'exécution de la loi ou soient nécessaires au bon exercice d'une activité autorisée par la Loi*;
b) l'utilisation des renseignements personnels soit faite en conformité avec le paragraphe 41 de la *LAIPVP* soit : *qu'une institution ne doit pas utiliser les renseignements personnels dont elle a la garde ou le contrôle, sauf selon certains cas prescrits par la Loi*;

c) le Collège applique une directive d'accès à l'information et de la vie privée conforme aux exigences de la *LAIPVP* dans toutes ses opérations;
d) cette directive respecte les principes de protection de la vie privée énoncés dans la *LAIPVP.*

Dans la présente directive, le terme « renseignements personnels » s'entend de tous les renseignements consignés ayant trait à un particulier qui peut être identifié, nonobstant le format dans lequel se trouve l'information (papier, électronique, vidéo, etc.). L'annexe A de la présente directive définit le terme « renseignements personnels » en conformité avec la *LAIPVP*.

---

2. DESTINATAIRES

La présente directive s'applique à tous les membres du personnel à temps plein et à temps partiel ainsi que les fournisseurs de services (ex. : services infonuagiques) et partenaires d'affaires (ex. : clinique de santé et association étudiante) qui ont accès à des renseignements personnels qui relèvent de la garde ou du contrôle du Collège.

La présente directive vise tous les renseignements personnels auxquels s'applique la *LAIPVP* et ayant trait à toute personne fréquentant le Collège ou ayant eu un rapport avec ce dernier, notamment les membres du personnel, la population étudiante présente, passée et future, les membres du Conseil d'administration, les membres de comités permanents ou temporaires, les corporations ou d'associations (association étudiante) ayant des liens directs avec le Collège ou relevant de son autorité, ainsi que les fournisseurs de services (services infonuagiques), les chercheurs, les visiteurs ou les invités qui n'ont pas de lien permanent avec le Collège.

---

3. MODALITÉS

À titre d'établissement d'enseignement désigné aux termes de la *LAIPVP,* le Collège est responsable des renseignements personnels qui sont sous sa garde et son contrôle, y compris les renseignements personnels qui sont communiqués par le Collège à des fournisseurs de services retenus par ce dernier.

Lorsqu'un fournisseur de services est retenu par le Collège, ce dernier s'assure qu'il existe des modalités suffisantes pour protéger les renseignements personnels qui seront partagés avec le fournisseur de services, notamment par l'entremise de dispositions particulières dans l'entente de services. Les renseignements personnels recueillis par le Collège pourraient, dans le cadre de la mise en œuvre des modalités de l'entente de services avec le fournisseur de services, être utilisés, divulgués ou hébergés par des fournisseurs de services situés ou dont les serveurs sont situés dans d'autres juridictions, dont les États-Unis d'Amérique ou en Europe, selon le cas.

Aux fins d'administration, la présidence-direction générale du Collège ainsi que la vice-présidence des Ressources humaines et culture organisationnelle ont des rôles distinctifs.

La présidence-direction générale du Collège a comme mandat de désigner une « personne responsable » de la *LAIPVP* et de la présente directive. Elle est responsable de l'approbation de la présente directive et des mises à jour. Elle voit à ce que la personne responsable implémente la présente directive au Collège et que les rapports soient complets.

La vice-présidence des Ressources humaines et culture organisationnelle est la personne responsable de la *LAIPVP* telle que désignée par la présidence-direction générale du Collège. Elle veille au respect des obligations du Collège conformément à la *LAIPVP*. Il incombe à la personne responsable de la directive sur l'accès à l'information et de la protection de la vie privée :

a. d'assurer le respect des diverses dispositions de la *LAIPVP* et de la directive sur l'accès à l'information et la protection de la vie privée;
b. de prendre connaissance, enregistrer et traiter toute demande d'accès à l'information présentée au Collège conformément à la *LAIPVP*;
c. de voir au déroulement du processus d'accès dans les délais prescrits;
d. de rassembler et revoir la documentation relative à la demande d'accès à l'information;
e. de préparer la correspondance nécessaire pour répondre aux exigences de la *LAIPVP*, notamment les exigences d'avis de confirmation ou refus de divulgation;
f. de déterminer le modèle de divulgation ainsi que l'entente d'utilisation de l'information s'y rattachant, le cas échéant.
g. de préparer la documentation à divulguer en réponse à une demande d'accès, y compris la « dé-identification » des renseignements personnels protégés par la *LAIPVP*. L'annexe B de la présente directive définit le terme « dé-identification » en conformité avec la *LAIPVP*;
h. de préparer le rapport annuel du Collège aux fins de remise au Commissaire à l'information et à la protection de la vie privée;
i. de coordonner et veiller à la mise en œuvre des mesures de formation du personnel en ce qui a trait aux exigences de la *LAIPVP*; et
j. de prélever les droits payables par l'auteur d'une demande d'accès à l'information conformément aux règlements pris en application de la *LAIPVP* et à la présente directive.

4. MODALITÉS PARTICULIÈRES

4.1. MODALITÉS CONCERNANT L'ACCÈS À L'INFORMATION

L'accès officiel à un document dont le Collège a la garde ou le contrôle passe par la présentation d'une demande écrite, accompagnée d'un montant initial de 5,00 $, à la personne responsable qui, sous réserve des exceptions prévues à la *LAIPVP*, voit à y répondre dans les trente (30) jours civils de sa réception.

Si un secteur reçoit directement une demande d'accès à l'information, il doit, sans délai, en informer la personne responsable. La personne responsable traite ensuite la demande en communiquant avec le secteur concerné, lequel coopère avec la personne responsable pour ce qui est du rassemblement de l'information pertinente.

La décision de donner accès à la totalité ou à une partie de l'information visée par la demande d'accès est prise par la personne responsable.

Une fois la décision prise, la personne responsable achemine la réponse du Collège à l'auteur de la demande d'accès, dans les trente (30) jours civils suivant la réception de la demande, sauf dans le cas des exceptions prévues par la *LAIPVP*; la réponse est accompagnée, s'il y a lieu, de l'information demandée ou des directives détaillées permettant à l'auteur de la demande de consulter la documentation originale.

Le Collège peut prélever des droits pour couvrir les frais de recherche, de préparation, de récupération, de traitement, de reproduction et d'expédition de l'information traitée et divulguée en rapport à une demande d'accès. Ces droits sont évalués et exigés conformément au règlement concernant les droits perçus en application de la *LAIPVP*.

4.2 MODALITÉS CONCERNANT LA PROTECTION DE LA VIE PRIVÉE ET LA CONSERVATION DES RENSEIGNEMENTS PERSONNELS

En vertu du paragraphe 39(1) de la *LAIPVP*, le Collège ne doit recueillir les renseignements personnels que directement du seul particulier concerné par ces renseignements, sauf si :

a. ce particulier a autorisé un autre mode de collecte;
b. leur divulgation à l'institution concernée est autorisée aux termes de l'article 42 ou de l'article 32 de la *Loi sur l'accès à l'information municipale et la protection de la vie privée*;
c. leur mode de collecte a reçu l'autorisation du commissaire en vertu de l'alinéa 59 c);
d. les renseignements sont consignés dans le rapport d'un organisme de renseignements au sens de la *Loi sur les renseignements concernant le consommateur*;
e. les renseignements sont recueillis aux fins de déterminer les candidats possibles à une distinction ou à un prix en reconnaissance de réalisations exceptionnelles ou de services éminents;
f. les renseignements sont recueillis aux fins d'une instance poursuivie ou envisagée devant soit un tribunal, soit un tribunal administratif;
g. les renseignements sont recueillis aux fins de l'exécution de la Loi;
h. un autre mode de collecte des renseignements est autorisé par une loi ou en vertu de celle-ci.

La divulgation se fera notamment en vertu du paragraphe 42(1) de la *LAIPVP*.

Outre son respect des dispositions législatives qui protègent contre la divulgation de renseignements personnels et gouvernent la conservation et la destruction de ces renseignements, le Collège prend toutes les mesures nécessaires pour prévenir contre les risques de divulgation non contrôlés des renseignements personnels en sa possession ou sous son contrôle, tels que le risque de vol; le risque d'accès, de divulgation ou de reproduction non autorisée; et le risque de modification ou de destruction non conforme aux exigences législatives. Le Collège entend maintenir cette protection pour tous les renseignements personnels en sa possession ou sous son contrôle, quelle qu'en soit la forme.

Tous les membres du personnel, agents, fournisseurs de services et bénévoles autorisés du Collège ayant accès aux renseignements personnels en la possession ou sous le contrôle du Collège sont tenus de respecter la confidentialité de ces renseignements. À cette fin, ils s'engagent, par écrit, à respecter le caractère confidentiel des informations disponibles dans le cadre de leur poste ou de leurs fonctions et participent à toute formation dispensée par le Collège en relation avec la *LAIPVP*.

L'annexe C sert d'aide-mémoire lors de la négociation d'un contrat ou d'une entente de services avec un fournisseur proposé.

Les personnes ayant accès aux renseignements personnels sont tenues de respecter, en tout temps, les mesures de protection mises en œuvre par le Collège, dont :

a. toute mesure physique, telle que le verrouillage des classeurs et l'accès restreint aux bureaux et aux salles d'entreposage;
b. toute mesure organisationnelle mise en œuvre pour restreindre l'accès aux personnes œuvrant au sein du Collège qui ont véritablement besoin d'accéder à ces renseignements personnels;
c. toute mesure technologique mise en œuvre par le Collège, telle que l'utilisation de mots de passe, de processus de vérification et d'encodage.

4.3 MODALITÉS CONCERNANT LA DIVULGATION DE RENSEIGNEMENTS PERSONNELS

Le Collège ne doit pas divulguer les renseignements dont il a la garde ou le contrôle, sauf :

a) tel que prescrit par la Loi;
b) aux fins pour lesquelles ils ont été obtenus ou recueillis;
c) dans le cadre de la négociation et de l'administration des diverses conventions collectives et conditions d'emploi régissant les membres du personnel des collèges;
d) à un administrateur, à un employé, ou à une tierce partie (comprenant notamment un représentant d'un fournisseur de services) du Collège à qui ces renseignements sont nécessaires dans l'exercice de leurs fonctions et que cette divulgation est essentielle et appropriée à l'acquittement des fonctions du Collège;
e) à un représentant du Collège, désigné par une directive par exemple, ou de la Loi dans le cadre d'une enquête;
f) lors d'une situation d'urgence pouvant avoir une incidence sur la santé et la sécurité d'un employé;
g) dans une situation relative à un événement majeur de nature personnelle afin de faciliter la communication avec les proches du particulier blessé, malade ou décédé;
h) avec l'autorisation écrite de la personne visée.

---

5. DIRECTIVES, POLITIQUES OU PROCÉDURES RELIÉES

DIRECTIVES ADMINISTRATIVES ASSOCIÉES

RH-02 Équité en matière d'emploi
RH-03 Avantages accessoires
ADM-10 Utilisation de l'infrastructure technologique

POLITIQUE(S) ASSOCIÉE(S) :

3.01 - Contraintes générales à la présidence du Collège
3.03 - Ressources humaines
3.06 - Protection des actifs

ANNEXE A - DÉFINITIONS

« Renseignements personnels »

Extrait tiré du Sommaire de la *Loi sur l'accès à l'information et la protection de la vie privée*

Définitions

2. *(1) Les définitions qui suivent s'appliquent à la présente loi.*

[…]

Renseignements personnels : renseignements consignés ayant trait à un particulier qui peut être identifié. S'entend notamment :

a) des renseignements concernant la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, le sexe, l'orientation sexuelle, l'état matrimonial ou familial de celui-ci;

b) des renseignements concernant l'éducation, les antécédents médicaux, psychiatriques, psychologiques, criminels ou professionnels de ce particulier ou des renseignements reliés à sa participation à une opération financière;

c) d'un numéro d'identification, d'un symbole ou d'un signe individuel qui lui est attribué;

d) de l'adresse, de numéro de téléphone, des empreintes digitales ou de groupe sanguin de ce particulier;

e) de ses opinions ou de ses points de vue personnels, sauf s'ils se rapportent à un autre particulier;

f) de la correspondance ayant explicitement ou implicitement un caractère personnel et confidentiel, adressé par le particulier à une institution, ainsi que des réponses à cette correspondance originale susceptibles d'en révéler le contenu;

g) des opinions et des points de vue d'une autre personne au sujet de ce particulier;

h) *du nom du particulier, s'il figure parmi d'autres renseignements personnels qui le concernent, ou si sa divulgation risque de révéler d'autres renseignements personnels au sujet du particulier. […]*

[…].

Renseignements sur l'identité professionnelle

(3) Les renseignements personnels excluent le nom, le titre, les coordonnées et la désignation d'un particulier qui servent à l'identifier par rapport à ses activités commerciales ou à ses attributions professionnelles ou officielles.

ANNEXE B – AUTRES DÉFINITIONS

Dé-identification

« Dé-identification » s'entend du terme général pour définir le processus d'élimination des renseignements personnels d'un fichier ou d'un ensemble de données. Plus précisément, la dé-identification se définit comme étant le processus d'élimination de toute information qui (i) identifie une personne ou qui (ii) prise seule ou en combinaison avec d'autres informations, pourrait raisonnablement identifier une personne.

Selon le processus de dé-identification, le Collège doit éliminer l'information qui identifie directement une personne et l'information qui, prise seule ou en combinaison avec d'autres informations, pourrait raisonnablement identifier une personne. Le premier type d'identifiant constitue un « identifiant direct », tandis que le second représente un « identifiant indirect » ou « quasi-identifiant ».

Identifiant direct

« Identifiant direct » s'entend d'une variable ou de plusieurs variables qui, prises seules ou en combinaison avec d'autres sources d'information facilement accessibles, permettent d'identifier une personne. Des exemples en sont les noms, les adresses, les adresses électroniques, les numéros de téléphone, les numéros de télécopieur, les numéros de carte de crédit, les numéros de plaque, les numéros d'identification de véhicule, les numéros d'assurance sociale, les numéros de carte santé, les numéros de dossier médical, les numéros d'identification d'un appareil, les identificateurs biométriques, les numéros d'adresse de protocole Internet et les adresses URL.

Identifiant indirect ou quasi-identifiant

« Identifiant indirect ou quasi-identifiant » s'entend de variables ayant deux caractéristiques importantes : (1) l'adversaire en a vraisemblablement une connaissance préalable et (2) elles peuvent être utilisées, seules ou en combinaison avec d'autres, pour ré-identifier une personne dans un ensemble de données. Des exemples en sont le sexe, la date de naissance ou l'âge, les dates d'évènement, les lieux, l'origine ethnique, le pays de naissance, les langues parlées, le statut d'autochtone, le statut de minorité visible, la profession, l'état civil, le niveau de scolarité, les années d'étude, les antécédents criminels, le revenu total et la confession religieuse.

Adversaire

« Adversaire » s'entend d'une personne ou d'une entité qui tente de ré-identifier une personne ou plus dans un ensemble de données.

ANNEXE C – AIDE-MÉMOIRE

Aide-mémoire lors de la négociation d'un contrat ou d'une entente de services avec un fournisseur proposé

Sommaire des mesures recommandées :

- Donner un préavis adéquat aux étudiants quant à l'utilisation possible de leurs renseignements personnels et de la possibilité que ceux-ci soient utilisés/hébergés dans des serveurs situés à l'étranger.

- Effectuer des recherches approfondies en lien avec le fournisseur de services. La vérification à entreprendre devrait être proportionnelle à l'étendue des renseignements personnels qui leur sera confiée, mais devrait inclure des renseignements de base, notamment :

    - L'adresse du siège social du fournisseur de services, le lieu précis du serveur qui hébergera les données en cause, une revue de la réputation du fournisseur de services, des renseignements sur les autres clients du fournisseur de services, des renseignements à savoir si le fournisseur de services est à risque d'être acheté par un compétiteur.
    - L'utilisation par le fournisseur de services de sous-traitants ou tierces parties à titre de mandataire dans le cadre de ses opérations habituelles.
    - Des renseignements sur les standards de sécurité du fournisseur de services en lien avec les services offerts.
    - Les modalités en lien avec les audits et les vérifications des mesures de sécurité mises en place par le fournisseur de services.

- Négocier les paramètres de l'entente de services avec le fournisseur de services responsable de l'hébergement des données afin de prévoir :

    - Une clause à l'effet que le fournisseur prendra toutes les mesures techniques, administratives et physiques qui s'imposent pour assurer la sécurité et la fiabilité des renseignements personnels qui lui sont confiés par le Collège, y compris pour empêcher l'utilisation ou la divulgation non autorisée à des tiers.
    - Une clause à l'effet que le fournisseur de services reconnaît que les obligations en matière d'accès à l'information et de protection à la vie privée du Collège sont prescrites par la *LAIPVP* et que le fournisseur de services s'engage à respecter les modalités de la *LAIPVP*, y compris en matière de collecte, conservation, utilisation et de divulgation des renseignements personnels.
    - Une clause selon laquelle le serveur hébergeant les données en cause et les données elles-mêmes ne peuvent être déplacées à un autre endroit physique que celui prévu dans l'entente de services sans qu'un préavis écrit soit fourni au Collège. Dans un tel cas, le Collège se réserve le droit d'exercer un droit de retrait dans l'éventualité où le Collège détermine, à son entière discrétion, que la destination pose un risque accru.
    - Une clause à l'effet que les renseignements personnels régis par l'entente ne seront, à aucun moment, hébergés sur des outils non chiffrés, y compris, mais sans toutefois s'y limiter, un CD-ROM, une clé USB ou tout autre outil non chiffrés semblable.
    - Une clause sur le protocole à suivre dans l'éventualité d'une fuite de renseignements personnels.
    - Une clause à l'effet que l'ensemble des renseignements personnels communiqués au fournisseur de services demeurent la propriété du Collège, ne lui sont communiqués que

pour les fins prévues par l'entente de services et ne peuvent être utilisés par le fournisseur de services pour toute autre fin. De même, le fournisseur de services doit s'engager à remettre l'ensemble des renseignements personnels une fois l'entente de services terminée et/ou à veiller à la destruction de ceux-ci à la satisfaction du Collège.

- Une clause à l'effet que le fournisseur de services ne puisse pas retenir les services d'un sous-traitant ou mandataire en lien avec les données en cause sans que le Collège reçoive un préavis à cet effet, que dans un tel cas, le sous-traitant accepte d'être lié par les mêmes modalités en matière de confidentialité que le fournisseur de services initial et que, le cas échéant, le Collège ait l'option d'annuler l'entente s'il détermine, à son entière discrétion, que le sous-traitant ou mandataire n'est pas adéquat.
- Une clause à l'effet que le Collège se réserve le droit de vérifier et d'inspecter (virtuellement ou en personne) les installations virtuelles ou physiques du fournisseur de services, y compris les moyens de traitement et de stockage employés par le fournisseur de services.
- Une clause d'indemnité pour le Collège pour toute dépense, frais juridiques ou autre frais associés aux gestes posés par le fournisseur de services, y compris par négligence.
- Une clause à l'effet que le fournisseur de services et son personnel n'accèderont pas aux renseignements personnels hébergés sur son serveur sauf dans la mesure où un tel accès est requis en vertu de l'entente de services ou pour des fonctions analogues. Dans la mesure où un accès est justifié, le fournisseur de services n'accèdera qu'aux renseignements personnels nécessaires dans les circonstances et y accédera uniquement pour les fins précitées. Avant que tout employé ou mandataire du fournisseur de services puisse accéder à quelconque renseignement personnel, le fournisseur de services doit s'assurer d'obtenir de sa part un engagement de confidentialité. Une copie de cet engagement signé doit, sur demande, être remise au Collège.
- Une clause exigeant la séparation des renseignements personnels relevant du Collège face aux autres renseignements hébergés sur le serveur du fournisseur de services.
- Une clause à l'effet que si le Collège reçoit une demande d'accès à l'information, le fournisseur de services s'engage à donner suite à toute demande du Collège découlant de celle-ci dans les plus brefs délais après en avoir reçu la demande du Collège. Dans le même sens, le fournisseur de services s'engage à coopérer avec toute enquête entamée par le Collège ou par le Commissaire à l'information et la protection de la vie privée de l'Ontario en lien avec les renseignements personnels visés par la présente entente.
- Une clause à l'effet que si le fournisseur de services reçoit une demande, ordonnance ou un mandat de perquisition ou de fouille quelconque, y compris en matière criminelle ou sécurité nationale, exigeant la divulgation des renseignements personnels visés par l'entente de services à un tiers (p. ex., une agence chargée de l'application de la Loi), le fournisseur de services doit aviser le Collège dans les plus brefs délais.
- Une clause permettant au Collège de mettre fin à l'entente ou de suspendre l'entente et obligeant le fournisseur de services de remettre toute donnée régie par l'entente au Collège ou d'en assurer la destruction à la satisfaction du Collège advenant le non-respect des modalités en matière de protection du droit à la vie privée prévue dans l'entente.
- Idéalement, une clause selon laquelle tout différend découlant de l'entente de services est sujet au droit et à la juridiction des tribunaux de l'Ontario.

Pour de plus amples renseignements sur les recommandations du Commissaire à l'information et à la protection de la vie privée de l'Ontario, veuillez consulter la publication suivante : *Thinking about Clouds? Privacy, security and compliance considerations for Ontario public sector institutions* (Feb. 2016) (disponible en anglais seulement).