CÉGEP DE VALLEYFIELD

Direction des affaires corporatives, du développement institutionnel et des communications

RECUEIL DE GESTION

TITRE: ***Politique encadrant la gouvernance à l'égard de la protection des renseignements personnels***

NUMÉRO : ***DACDIC-23-PO-01***

Responsable de l'application

- [ ] *Président du conseil d'administration*
- [ ] *Direction générale*
- [ ] *Direction de la formation continue*
- [ ] *Direction des études*
  - [ ] *Service du développement pédagogique et de l'encadrement scolaire*
  - [ ] *Service de l'organisation scolaire*
- [ ] *Direction des ressources humaines*
- [ ] *Direction des services administratifs*
  - [ ] *Service des finances*
  - [ ] *Service des ressources matérielles et des services communautaires*
  - [ ] *Service de l'approvisionnement*
- [ ] *Direction des technologies de l'information*
- [ ] *Direction des affaires étudiantes*
- [X] *Direction des affaires corporatives, du développement institutionnel et des communications*

Destinataires

- *Toute personne physique ou morale du Cégep faisant la collecte et/ou l'usage de renseignements personnels dans le cadre de ses activités*

Approuvé par

- *Conseil d'administration*

Document de référence

Mise en application

- *Adoption : 24 octobre 2023*
- *Entrée en vigueur : 24 octobre 2023*
- *Révision :*
- *Modification :*

INTRODUCTION

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[1] (ci-après la « Loi 25 ») actualise l'encadrement applicable à la protection des renseignements personnels, dont la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[2] (ci-après la « Loi sur l'accès »).

Le Cégep est désormais tenu d'adopter et d'assurer l'application d'une politique en lien avec les règles encadrant la gouvernance à l'égard de la protection des renseignements personnels qu'il détient.

La présente politique est complémentaire à la *Politique sur la sécurité de l'information* existante au Cégep depuis le 24 octobre 2023.

ARTICLE 1 – OBJECTIFS DE LA POLITIQUE

La présente politique a pour objectif d'affirmer l'engagement du Cégep à s'acquitter pleinement de ses obligations à l'égard de la protection des renseignements personnels, quels que soient leurs supports ou leurs moyens de communication.

Plus précisément, le Cégep doit veiller à la confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.

ARTICLE 2 – CADRE LÉGAL ET NORMATIF

En tant qu'organisme public, le Cégep recueille des renseignements personnels, notamment ceux de la population étudiante et des membres du personnel. Il est donc assujetti aux dispositions de la Loi sur l'accès, au *Code civil du Québec*[3] et à la *Charte des droits et libertés de la personne*[4]. En cas de divergence entre la Loi sur l'accès et la présente politique, la Loi sur l'accès prévaut.

En cas de divergence entre les modalités contenues aux règlements, politiques, directives et procédures du Cégep concernant les renseignements personnels, les règles de la présente directive prévalent.

ARTICLE 3 – CHAMP D'APPLICATION DE LA POLITIQUE

La présente s'applique à toute personne qui, dans l'exercice de ses fonctions, collecte, consulte, utilise, communique, détient ou conserve des renseignements personnels détenus par le Cégep concernant toute personne physique. Les renseignements visés sont ceux que le Cégep détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers.

[1] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, L.Q. 2021, c. 25

[2] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1

[3] *Code civil du Québec*, c. CCQ-1991

[4] *Charte des droits et libertés de la personne*, RLRQ, c. C-12

ARTICLE 4 - DÉFINITIONS

Dans la présente politique, à moins que le contexte ne s'y oppose, les expressions suivantes signifient :

Communauté collégiale : La communauté collégiale comprend les membres du personnel, les étudiant(e)s et les bénévoles.

Confidentialité : propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes ou entités désignées et autorisées.

Consentement : Le consentement est l'autorisation de la personne titulaire des renseignements personnels à recueillir et utiliser 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.

Cycle de vie de l'information : l'ensemble des étapes que parcourt une information, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation du Cégep.

Direction des technologies de l'information (DTI) : Directeur TI et son équipe, mandatée pour gérer les flux de données, pour installer des équipements et des logiciels, pour entretenir et développer des réseaux informatiques et pour protéger les actifs informationnels et les données conservées sur les serveurs du Cégep ou ailleurs.

Fournisseur : Personne ou établissement qui fournit au cégep des marchandises ou des services.

Majeur : Personne âgée de 18 ans et plus ou personne âgée de moins de 18 ans émancipée.

Mineur : Personne âgée de moins de 18 ans.

Membre du personnel : toute personne salariée, syndiquée ou non, incluant les cadres et les hors cadres, les travailleurs et travailleuses autonomes ainsi que les sociétés en nom collectif sous contrat avec le Cégep**.**

Renseignement personnel : Tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier, tel que : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, l'occupation, le numéro d'assurance sociale, la date de naissance, la photographie et les coordonnées bancaires. Les renseignements personnels doivent être protégés, peu importe la nature de leur support et quelle que soit leur forme : écrite, graphique, sonore, visuelle, informatisée ou autre.

Renseignement personnel sensible : Un renseignement personnel est sensible lorsque, par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée[5]. Sont, notamment, considérés comme sensibles les renseignements suivants : des renseignements médicaux, biométriques, génétiques ou financiers, ou encore des renseignements sur la vie ou l'orientation sexuelle, les convictions religieuses ou bien l'origine ethnique[6].

[5] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, RLRQ 2021, C.25, art. 59.

[6] Gouvernement du Québec (2023). *Définition de mots en lien avec la protection des renseignements personnels*, URL : https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/definitions-concepts/lexique

ARTICLE 5 : COLLECTE DES RENSEIGNEMENTS PERSONNELS

5.1 Renseignements personnels pouvant être collectés

Afin de remplir adéquatement sa mission, le Cégep doit recueillir plusieurs renseignements personnels.

Celui-ci recueille uniquement les renseignements personnels nécessaires à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion.

Dans certaines situations précises, le Cégep peut également recueillir un renseignement personnel si celui-ci est nécessaire à la mise en œuvre d'un programme d'un organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune. Dans certains cas, la collecte doit être précédée d'une évaluation des facteurs relatifs à la vie (ÉFVP) privée et s'effectuer dans le cadre d'une entente écrite transmise à la Commission d'accès à l'information du Québec conformément à la Loi sur l'accès.

Le Cégep prend des mesures pour s'assurer que les renseignements personnels qu'il recueille sont adéquats, pertinents, non excessifs et utilisés à des fins limitées.

5.2 Informations communiquées lors de la collecte de renseignements personnels

Lorsqu'il recueille des renseignements personnels, le Cégep s'assure d'informer la personne concernée, au plus tard au moment de la collecte :

1. Du nom de l'organisme public au nom de qui la collecte est faite ;
2. Des fins auxquelles ces renseignements sont recueillis ;
3. Des moyens par lesquels les renseignements sont recueillis ;
4. Du caractère obligatoire ou facultatif de la demande ;
5. Des conséquences d'un refus de répondre ou de consentir à la demande ;
6. Des droits d'accès et de rectification prévus par la loi ;
7. De la possibilité que les renseignements personnels soient communiqués à l'extérieur du Québec, le cas échéant.

Sur demande, la personne concernée est également informée des renseignements personnels recueillis auprès d'elle, des catégories de personnes qui y ont accès au sein de l'organisme public, de la durée de conservation de ces renseignements ainsi que des coordonnées de la personne responsable de la protection des renseignements personnels.

ARTICLE 6 : UTILISATION DES RENSEIGNEMENTS PERSONNELS

Le Cégep utilise des renseignements personnels concernant sa clientèle étudiante, les membres de son personnel et d'autres tierces parties afin de s'acquitter de sa mission et de ses fonctions. Il ne fera pas usage des renseignements personnels à d'autres fins que celles précisées lors de la collecte, à moins d'avoir obtenu un consentement de la ou des personnes concernées ou que la Loi sur l'accès l'exige.

ARTICLE 7 : CONSENTEMENT

Dans les situations qui le requièrent, le Cégep devra transmettre un consentement à la cueillette, à l'utilisation ou à la divulgation des renseignements personnels aux personnes concernées. Pour être

valable, le consentement devra être manifeste, libre, éclairé, être donné à des fins spécifiques, en termes simples et clairs ainsi que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.

Lorsqu'une personne a donné son consentement à la collecte, à l'utilisation et à la communication de ses renseignements personnels, elle peut le retirer à tout moment. Pour retirer son consentement, le cas échéant, elle peut communiquer avec la personne dont le nom est indiqué dans le formulaire de consentement (par exemple : par courriel, télécopieur, téléphone, etc.).

Veuillez noter que si une personne retire son consentement, il se peut que le Cégep ne puisse pas fournir un service particulier. Par exemple, le candidat qui refuse de donner son consentement pour la transmission de ses notes du secondaire au Cégep pourrait ne pas être admis. Le Cégep expliquera à cette personne l'impact du retrait de son consentement pour l'aider dans sa prise de décision.

Voir Annexe A pour un exemple de formulaire de consentement.

ARTICLE 8 : COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

8.1 Communication sans le consentement de la personne concernée

Le Cégep peut divulguer 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 s'il croit que la divulgation est nécessaire ou appropriée pour protéger les droits, la propriété ou la sécurité du Cégep ou d'autres personnes.

Le Cégep peut communiquer certains renseignements personnels qu'il détient à un membre du personnel du Cégep qui a la qualité pour le recevoir et lorsque ce renseignement est nécessaire à l'exercice de ses fonctions.

Le Cégep peut transférer les renseignements personnels qu'il collecte à des fournisseurs de services et à d'autres tiers qui le soutiennent dans sa mission. Ces tiers sont contractuellement obligés de garder les renseignements personnels confidentiels, de les utiliser uniquement aux fins pour lesquelles le Cégep les divulgue et de traiter les renseignements personnels selon les normes énoncées dans la politique et en respect des lois.

Le Cégep 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 sur l'accès dont, notamment, l'évaluation des facteurs relatifs à la vie privée et la transmission de l'entente à la Commission d'accès à l'information trente (30) jours avant son entrée en vigueur[7].

Dans certaines situations, la personne responsable de la protection des renseignements personnels doit inscrire la communication dans son registre de communication des renseignements personnels.

[7] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, L.Q. 2021, c. 25, art. 67.2.1 à 67.2.3

Les exceptions à la communication ou à l'utilisation des renseignements personnels qui doivent être inscrites au registre de communication des renseignements personnels sont décrites dans l'Annexe B.

8.2 Communication avec le consentement de la personne concernée

Le Cégep peut communiquer certains renseignements personnels détenus à une personne s'il a obtenu le consentement valable de la personne concernée.

ARTICLE 9 : CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

Le Cégep ne conserve les renseignements personnels qu'il détient que pour le temps nécessaire pour atteindre les fins pour lesquelles il les a collectés et conformément à son calendrier de conservation, à moins d'autorisation ou d'exigence des lois ou de la réglementation applicable.

En règle générale, lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, le Cégep doit le détruire ou l'anonymiser pour l'utiliser à des fins d'intérêt public.

Un renseignement concernant une personne physique est anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus d'identifier directement ou indirectement cette personne. Il convient de noter que le processus d'anonymisation doit être irréversible.

Cependant, par exception à la règle générale, s'il s'agit de renseignements personnels contenus dans un document visé par le calendrier de conservation du Cégep, celui-ci doit respecter les règles qui y sont prévues en matière de conservation et de destruction de ces documents.

Lorsque le Cégep procède à la destruction de documents contenant des renseignements personnels, il 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.

Les renseignements personnels détenus par le Cégep sont traités et stockés au Québec. Dans l'éventualité où un transfert de renseignements personnels à l'extérieur du Québec serait nécessaire dans le cadre de l'exercice des fonctions du Cégep, ce transfert n'aura 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.

ARTICLE 10 : PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le Cégep a mis en place des mesures de sécurité physiques, organisationnelles, contractuelles et technologiques appropriées et raisonnables afin de protéger les renseignements personnels recueillis contre la perte ou le vol, et contre l'accès, la divulgation, la copie, l'utilisation ou la modification non autorisés par la loi. Le Cégep a pris des mesures pour faire en sorte que seuls les membres du

personnel qui doivent absolument avoir accès aux renseignements personnels recueillis dans le cadre de leurs fonctions soient autorisés à y accéder.

Les personnes qui travaillent pour le Cégep ou en son nom doivent, notamment :

- Fournir des efforts raisonnables pour minimiser le risque de divulgation non intentionnelle de renseignements personnels ;
- Prendre des précautions particulières pour s'assurer que les renseignements personnels ne sont pas surveillés, entendus, consultés ou perdus lorsqu'elles travaillent dans des locaux autres que les bureaux du Cégep ; et
- Prendre des mesures raisonnables pour protéger les renseignements personnels lorsqu'elles se déplacent d'un endroit à l'autre.

Les sous-traitants ayant accès aux renseignements personnels dont le Cégep a la garde ou le contrôle seront informés de la présente politique de protection des renseignements personnels et des autres politiques et processus applicables pour assurer la sécurité et la protection des renseignements personnels. Tous les sous-traitants devront s'engager par écrit à accepter de se conformer aux politiques, aux processus et aux lois applicables.

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

11.1 Demande d'accès à ses renseignements personnels

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

Une demande de communication 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 du Cégep, soit la Direction des affaires corporatives, du développement institutionnel et des communications. La demande doit fournir suffisamment d'indications précises pour permettre au Cégep de la traiter.

La personne responsable de la protection des renseignements personnels doit donner à la personne qui lui a fait une demande écrite un avis de la date de la réception de sa demande.

La personne responsable doit répondre au plus tard dans les vingt (20)[8] jours qui suivent la date de la réception d'une demande. Si le traitement de la demande dans le délai prévu précédemment ne lui paraît pas possible sans nuire au déroulement normal des activités du Cégep, la personne responsable peut, avant l'expiration de ce délai, le prolonger d'une période n'excédant pas dix (10) jours en donnant un avis à cet effet à la personne requérante avant l'expiration du délai de vingt (20) jours.

[8] Loi sur l'accès, article 47.

Si la personne qui fait la demande n'est pas satisfaite de la réponse du Cégep, elle peut saisir la Commission d'accès à l'information de cette décision afin que celle-ci soit révisée. Cette demande de révision 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 sur l'accès pour répondre à la demande.

Le Cégep n'impose pas l'utilisation d'un formulaire pour présenter une demande d'accès à un document. Toutefois, la personne qui le souhaite peut utiliser le formulaire proposé par la Commission d'accès à l'information du Québec :

Formulaire de demande d'accès CAI

La procédure pour présenter la demande et la traiter est également décrite sur le site Web de la Commission d'accès à l'information :

Accéder aux documents des organismes publics

11.1 Demande de rectification

Toute personne qui reçoit 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 sur l'accès, 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 adressée à la personne responsable de la protection des renseignements personnels du Cégep, soit la Direction des affaires corporatives, du développement institutionnel et des communications. La demande doit fournir suffisamment d'indications précises pour permettre au Cégep de la traiter.

Le Cégep doit, lorsqu'il accède à une demande de rectification d'un fichier, délivrer sans frais à la personne qui l'a faite une copie de tout renseignement personnel modifié ou ajouté, ou, selon le cas, une attestation du retrait d'un renseignement personnel.

Lorsque le Cégep 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.

La personne responsable doit répondre au plus tard dans les vingt (20) jours qui suivent la date de la réception d'une demande. Si le traitement de la demande dans le délai prévu précédemment ne lui paraît pas possible sans nuire au déroulement normal des activités du Cégep, la personne responsable peut, avant l'expiration de ce délai, le prolonger d'une période n'excédant pas dix (10) jours en donnant un avis à cet effet à la personne requérante.

Si la personne qui fait la demande n'est pas satisfaite de la décision du Cégep, elle peut saisir la Commission d'accès à l'information de cette décision afin que celle-ci soit révisée. Cette demande de révision 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 sur l'accès pour répondre à la demande.

Le Cégep n'impose pas l'utilisation d'un formulaire pour présenter une demande de rectification. Toutefois, la personne qui le souhaite peut utiliser le formulaire proposé par la Commission d'accès à l'information du Québec :

Demande de rectification CAI

ARTICLE 12 : GESTION DES INCIDENTS DE CONFIDENTIALITÉ

12.1 Définition

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

1. L'accès non autorisé par la Loi sur l'accès à un renseignement personnel ;
2. L'utilisation non autorisée par la Loi sur l'accès d'un renseignement personnel ;
3. La communication non autorisée par la Loi sur l'accès d'un renseignement personnel ;
4. La perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Pour des exemples concrets d'incidents de confidentialité, voir Annexe C.

12.2 Traitement d'un incident de confidentialité

Lorsque le Cégep a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient, il 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, ce qui peut inclure la sanction des individus en cause.

Le Cégep peut également aviser toute personne et/ou tout organisme susceptible 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 enregistrer la communication.

Si l'incident de confidentialité présente un risque qu'un préjudice sérieux soit causé, l'organisme doit, avec diligence, en aviser la Commission. Il doit également aviser toute personne dont un renseignement personnel est concerné par l'incident.

Afin d'évaluer le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, le Cégep doit considérer, notamment :

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

Le Cégep doit également consulter la personne responsable de la protection des renseignements personnels.

12.3 Registre des incidents de confidentialité (Voir Annexe D)

Un organisme public doit tenir un registre des incidents de confidentialité. Celui-ci contient, notamment :

1. Une description des renseignements personnels visés par l'incident ;
2. Les circonstances de l'incident ;
3. La date où l'incident a eu lieu ;

4. La date où la personne responsable de la protection des renseignements personnels a eu connaissance de l'incident ;
5. Le nombre de personnes visées ;
6. L'évaluation de la gravité du risque de préjudice ;
7. S'il existe un risque de préjudice sérieux pour la personne concernée, les dates de transmission des avis ; et
8. Les mesures prises en réaction à l'incident.

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

Toute personne qui a des motifs de croire qu'un incident de confidentialité s'est produit et que le Cégep a fait défaut de protéger la confidentialité des renseignements personnels qu'il détient peut déposer une plainte pour demander que la situation soit corrigée, conformément à la *Politique de service à la clientèle et de gestion des plaintes,* à la procédure de gestion des plaintes du Cégep et au formulaire prévu, en annexe, à cet effet.[9]

Le formulaire de plainte relative à la protection des renseignements personnels est disponible à la Direction des affaires corporatives, du développement institutionnel et des communications (dacdic@cegepvalleyfield.ca). Selon la nature et la portée de la plainte, la DACDIC pourra s'associer à un ou des membres du CAIPRP.

Une plainte en matière de protection de renseignements personnels peut porter sur la cueillette, la conservation, l'utilisation, la communication ou la destruction des renseignements personnels.

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

La plainte doit être déposée par écrit et 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 adressée à la personne responsable de la protection des renseignements personnels, soit la directrice ou le directeur de la DACDIC, dont les coordonnées sont diffusées sur le site Web du Cégep.

Dans le cas où la plainte met en cause la conduite de la personne responsable de la protection des renseignements personnels, celle-ci doit être adressée à la Directrice générale ou au Directeur général du Cégep.

13.1 Traitement de la plainte

La personne responsable de la protection des renseignements personnels ou la Directrice générale ou le Directeur général, le cas échéant, en collaboration si requis avec les membres du Comité sur l'accès à l'information et la protection des renseignements personnels, a la responsabilité de traiter la plainte dans un délai de 30 jours ouvrables.

[9] Cégep de Valleyfield (2010). *Politique de service à la clientèle et de gestion des plaintes*, URL : https://www.cegepvalleyfield.ca/wp-content/uploads/2023/04/ag-10-po-08_service-clientele-et-gestion-plaintes-originale-9-fevrier-2010.pdf

Dans le cas où celle-ci s'avère fondée, le Cégep prend les mesures requises pour corriger la situation dans les meilleurs délais conformément au paragraphe 12.2 de la présente politique et procède à l'inscription de l'incident au registre, comme indiqué au paragraphe 12.3.

Un retour est par la suite effectué à la personne ayant déposé la plainte pour lui faire part des mesures mises en place pour corriger la situation.

ARTICLE 14 : VIDÉOSURVEILLANCE

Le Cégep se dotera d'une *Directive portant sur la mise en place et l'utilisation d'un système de vidéosurveillance.* Le recours à la vidéosurveillance s'effectuera ainsi en respect des obligations prévues notamment par le *Code civil du Québec,* par la *Charte des droits et libertés de la personne* ainsi que par la Loi sur l'accès.

ARTICLE 15 : PROJETS DE SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE DE SERVICES IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS

Le Cégep procède à une évaluation des facteurs relatifs à la vie privée pour tout projet d'acquisition, de développement ou de refonte d'un système d'information ou d'une prestation électronique de services qui impliquerait la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

En ce qui concerne l'évaluation des facteurs relatifs à la vie privée, le Cégep consulte, dès le début du projet, son comité sur l'accès à l'information et la protection des renseignements personnels.

ARTICLE 16 : RÔLES ET RESPONSABILITÉS

La présente politique attribue l'application des règles de gouvernance en matière de protection des renseignements personnels du Cégep à des comités et à des personnes en raison des fonctions particulières qu'elles exercent et ce, tout au long du cycle de vie du renseignement personnel (de la collecte à la destruction).

16.1 Comité de gestion (cadres et hors-cadres)

En appui à la DACDIC, le Comité de gestion du Cégep veille à l'application de la *Politique encadrant la gouvernance à l'égard de la protection des renseignements personnels*, ainsi que toute modification à celle-ci. Le Comité de gestion offre son soutien à la personne responsable de la protection des renseignements personnels quant à son rôle et à l'exercice de ses attributions.

Ainsi, chaque cadre et hors-cadre :

- Informe le personnel sous son autorité et les tiers avec lesquels il fait affaire de la *Politique encadrant la gouvernance à l'égard de la protection des renseignements personnels* dans le but de les sensibiliser à la nécessité de s'y conformer ;
- Voit à la protection des renseignements personnels et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel sous son autorité en conformité avec la présente directive ;

- S’assure que les exigences en matière de protection des renseignements personnels sont prises en compte dans tout contrat de service sous sa responsabilité et voit à ce que tout consultant, fournisseur, partenaire, organisme ou firme externe s’engage à respecter la présente directive ;
- Rapporte à la personne responsable de la protection des renseignements personnels toute menace à la protection des renseignements personnels ou tout incident de confidentialité ;
- Collabore à la mise en œuvre de toute mesure visant à améliorer la protection des renseignements personnels ou à remédier à un incident de confidentialité.

16.2 Comité sur l’accès à l’information et la protection des renseignements personnels (CAIPRP)

Le comité sur l’accès à l’information et la protection des renseignements personnels veille à soutenir la direction générale dans l’exercice de ses responsabilités et dans l’exécution de ses obligations énoncées dans la *Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels* et la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*.

Le comité relève de la personne ayant la plus haute autorité au sein de l’organisme, soit la personne titulaire de la Direction générale.

Le CAIPRP se compose de :

- la personne responsable de l’accès aux documents ;
- la personne responsable de la protection des renseignements personnels ;
- toute autre personne dont l’expertise est requise, incluant, le cas échéant, le responsable de la sécurité de l’information et le responsable de la gestion documentaire.

Le CAIPRP exerce également les fonctions qui lui sont confiées par les deux lois mentionnées :

- Soutenir la personne responsable de la protection des renseignements personnels dans l’exercice de ses responsabilités et dans l’exécution de ses obligations ;
- Définir et approuver les orientations en matière de protection des renseignements personnels :
    - Rôles et responsabilités du personnel « tout au long du cycle de vie » des renseignements personnels ;
    - Processus de traitement internes des plaintes ;
    - Description des activités de formation et de sensibilisation offertes au personnel ;
    - Mesures de protection à l’égard des sondages.
- Approuver les règles de gouvernance à l’égard de la protection des renseignements personnels ;
- Rendre un avis et suggérer des mesures de protection sur tout projet d’acquisition. De développement et de refonte de système d’information ou de prestation électronique de services, incluant la vidéosurveillance et l’instauration d’une nouvelle technologie, impliquant la collecte, l’utilisation, la communication, la conservation ou la destruction de renseignements personnels ;
- Planifier et assurer la réalisation des activités de sensibilisation et de formation ;
- Promouvoir les orientations, les directives et les décisions formulées par la Commission d’accès à l’information (CAI) ;
- Évaluer annuellement le niveau de protection des renseignements personnels ;

- Rédiger et diffuser une politique de confidentialité en termes simples et clairs et en assurer la révision périodique ;
- Veiller à l'application de la *Politique de confidentialité* et la présente politique ;
- Utiliser des moyens qui assurent la protection des renseignements personnels dès leur conception (art. 63.7) (*Privacy by design – Respect de la vie privée assurée dès la conception*) ;
- En cas d'incident de confidentialité[10] présentant un risque de préjudice sérieux, obligation d'aviser :
    - La Commission d'accès à l'information (CAI) ;
    - La personne concernée.

16.3 Conseil d'administration

Le conseil d'administration adopte la *Politique encadrant la gouvernance à l'égard de la protection des renseignements personnels* ainsi que toute modification à celle-ci. Le conseil est tenu informé des actions du Cégep en lien avec la présente politique.

16.4 Direction générale (DG)

La DG :

- Assume le processus de délégation du rôle de responsable de la protection des renseignements personnels. Ce rôle est délégué à la Direction des affaires corporatives, du développement institutionnel et des communications (DACDIC) ;
- Approuve les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité et les redditions de comptes en matière de protection de renseignements personnels ;
- Veille à ce que le conseil d'administration soit informé, au moment opportun, des actions du Cégep en matière de protection de renseignements personnels en lien avec la présente politique ;
- Encadre le responsable de la protection des renseignements personnels dans la réalisation de son mandat ;
- Demeure imputable en matière de protection de renseignements personnels même après avoir délégué le rôle de responsable de la protection de renseignements personnels.

16.5 Direction des affaires corporatives, du développement institutionnel et des communications (DACDIC)

À titre de responsable de la gestion documentaire et des archives, la DACDIC :

- Déléguée par la Direction générale, agit comme responsable de la protection des renseignements personnels ;
- Sert de point de contact central pour la réception de toute plainte relativement à la protection des renseignements personnels ;

[10] La loi définit l'incident de confidentialité comme étant l'accès non autorisé par la loi à un renseignement personnel, l'utilisation ou la communication non autorisée par la loi d'un tel renseignement, la perte de ce renseignement ou toute autre atteinte à sa protection. Cet incident, impliquant des renseignements personnels, représente un risque sérieux d'atteinte à la vie privée d'un membre de la communauté collégiale.

- A la garde du registre des incidents de confidentialité et de tout autre document en lien avec la protection des renseignements personnels, notamment le formulaire de plainte et les différents formulaires de consentement ;
- Consulte, selon l'évaluation de la situation, un ou des membres du CAIPRP ;
- Veille à ce que le CAIPRP soit informé des actions du Cégep en matière de protection des renseignements personnels (reddition de compte annuelle ou bisannuelle).

16.6 Responsable de la protection des renseignements personnels

Au Cégep de Valleyfield, la responsabilité de cette charge incombe à la personne occupant la fonction de directeur ou directrice à la DACDIC. La personne responsable de la protection des renseignements personnels est chargée de l'application de la présente politique. Elle est notamment responsable de recevoir les plaintes, de faire les vérifications et analyses qui s'imposent et d'y répondre dans les délais requis.

Plus spécifiquement, la personne responsable de la protection des renseignements personnels (PRP) :

- Formule des recommandations au comité de direction du Cégep et au CAIPRP concernant les orientations, les initiatives et les bonnes pratiques en matière de PRP ;
- Assure la coordination et la cohérence des actions menées au sein du Cégep en matière de PRP ;
- Produit les redditions de comptes du Cégep en matière de PRP, au besoin ;
- Propose des dispositions visant le respect des exigences en matière de PRP à intégrer dans les ententes de services et les contrats, le cas échéant ;
- S'assure de la déclaration par le Cégep des incidents de confidentialité à la Commission d'accès à l'information (CAI) ;
- Élabore des activités de sensibilisation et de formation en matière PRP, au besoin, de concert avec les Ressources humaines, et veille au déploiement de celles-ci ;
- S'assure des veilles normatives, juridiques et gouvernementales afin de suivre l'évolution des normes, des lois et règlements et des pratiques gouvernementales en matière de PRP ;
- Assume toute autre responsabilité définie dans la présente directive.

16.7 Direction des technologies de l'information (DTI)

La DTI :

- Met toutes les mesures technologiques en œuvre pour protéger les renseignements personnels, notamment en respectant la *Politique de sécurité de l'information* ;
- En appui au responsable de la protection des renseignements personnels, fournit les outils pour recueillir les informations nécessaires au traitement d'une plainte en lien avec la protection des renseignements personnels.

16.8 Chef de la sécurité de l'information organisationnelle (CSIO)

La personne assumant la fonction de CSIO est un membre du personnel d'encadrement d'un organisme public. La fonction de CSIO est déléguée par la direction générale.

Le Chef de la sécurité de l'information organisationnelle :

- Assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation.

- Contribue à la mise en œuvre du cadre de gouvernance qui régit la sécurité de l'information au sein de son organisation, notamment en siégeant sur le comité CAIPRP et en respectant ses responsabilités décrites dans la *Politique de sécurité de l'information*.
- Est responsable de la diffusion et de la mise en application de la politique.

16.9 Direction des études (DÉ) et Direction de la formation continue (DFC)

La DÉ et la DFC :

- Doit informer tout nouvel étudiant du Cégep de la présente politique ;
- Doit gérer le ou le(s) formulaire(s) de consentement des étudiants, en collaboration avec la DACDIC ;
- Doit désigner au moins une personne pour faire partie du CAIPRP.

16.10 Direction des ressources humaines

La Direction des ressources humaines :

- Doit informer et obtenir de tout nouvel employé du Cégep son engagement au respect de la présente politique ;
- Doit désigner au moins une personne pour faire partie du CAIPRP.

16.11 Membres du personnel ayant accès à des renseignements personnels

Toute personne qui, dans le cadre de ses fonctions, accède à un renseignement personnel, le consulte, ou le traite est responsable de l'utilisation qu'elle en fait et doit procéder de manière à protéger ces renseignements.

À cette fin, la personne doit :

- Se conformer à la présente politique et à toute autre règle en matière de protection des renseignements personnels ;
- Utiliser les droits d'accès qui lui sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés ;
- Signaler à son supérieur immédiat tout incident de confidentialité, toute contravention à la présente politique, ou toute menace à la protection des renseignements personnels ;
- Collaborer à la mise en œuvre de toute mesure visant à améliorer la protection des renseignements personnels ou à remédier à un incident de confidentialité.

ARTICLE 17 : ACTIVITÉS DE FORMATION ET DE SENSIBILISATION À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS OFFERTES PAR L'ORGANISME À SON PERSONNEL

Telle que stipule la *Loi sur l'accès*, le Cégep offrira des activités de sensibilisation et de formation seront offertes à sa communauté collégiale en fonction des besoins et sous différentes formes.

Les activités seront diffusées sur les différentes plateformes du Cégep.

ARTICLE 18 : SANCTIONS APPLICABLES EN CAS DE NON-RESPECT DE LA PRÉSENTE POLITIQUE

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

Dans le cadre de ses relations contractuelles avec un tiers, le Cégep pourra mettre fin à tout contrat sans préavis pour non-respect de la présente politique. Celle-ci sera présentée à tous les tiers contractants avec le Cégep, lesquels devront s'engager, par écrit, à s'y conformer.

ARTICLE 19 : FORMATION, SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur l'adoption des comportements sécuritaires et sur la responsabilisation individuelle.

À cet égard, les membres de la communauté du Cégep doivent être sensibilisés :

- À la sécurité de l'information et des systèmes d'information du Cégep ;
- Aux conséquences d'une atteinte à la sécurité ;
- À leurs rôles et à leurs responsabilités en la matière.

Les organisations s'engagent sur une base régulière à sensibiliser et à former les utilisatrices et les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité de ces actifs ainsi qu'à leur rôle et leurs obligations en la matière. L'utilisatrice et l'utilisateur ont la responsabilité de participer à ces activités de sensibilisation et de formation. Par ailleurs, les organisations favorisent le recours aux services communs de formation en sécurité de l'information.

ARTICLE 20 : DIFFUSION ET MISE À JOUR DE LA POLITIQUE

La personne responsable de la protection des renseignements personnels, assistée du CAIPRP, s'assure de la diffusion et de la mise à jour de la politique déposée dans le recueil de gestion et ensuite diffusée sur le site Web et Omnivox.

ARTICLE 21 : RESPONSABILITÉ DE L'APPLICATION ET RÉVISION DE LA POLITIQUE

La personne responsable de la protection des renseignements personnels est responsable de l'application de la politique et de sa révision aux trois ans.

ARTICLE 22 : ENTRÉE EN VIGUEUR DE LA POLITIQUE

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration. Elle abroge et remplace la *Politique de Sécurité de l'information, d'utilisation des ressources informationnelles et de protection des renseignements personnels* AG-18-PO-11.

ANNEXE A :

EXEMPLE DE FORMULAIRE DE CONSENTEMENT RELATIF A LA COMMUNICATION DE RENSEIGNEMENTS PERSONNELS

Dans le cadre de [indiquer le contexte spécifique], j'ai divulgué différents renseignements personnels nécessaires au traitement de cette demande.

Je comprends que, conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, le Cégep requiert mon autorisation quant à la transmission de renseignements personnels me concernant et qui sont requis afin de [indiquer la fin spécifique].

Pour cette fin spécifique, j'autorise le Cégep à communiquer les renseignements personnels suivants me concernant : mon adresse courriel, mon numéro de téléphone, ma signature et mon numéro d'admission [indiquer de manière précise quels renseignements sont visés] à [indiquer de manière précise les personnes ou les entreprises à qui la transmission sera faite], et ce, de manière écrite.

Ce consentement est valide pour la durée de mes études au Cégep [indiquer la durée de validité du consentement].

Je comprends que ce consentement peut être modifié ou révoqué en tout temps. Pour ce faire, j'aurai à en informer une représentante ou un représentant du Cégep.

Signature de la personne étudiante	Nom en lettres moulées	Date

Annexe B

EXCEPTIONS A LA COMMUNICATION OU A L'UTILISATION DES RENSEIGNEMENTS PERSONNELS QUI DOIVENT ETRE INSCRITES AU REGISTRE DE COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

- À l'article 59 (1° à 4°) ;

  1° Au procureur du Cégep si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi que le Cégep est obligé d'appliquer, ou au Directeur des poursuites criminelles et pénales si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec ;

  2° Au procureur du Cégep, ou au procureur général lorsqu'il agit comme procureur du Cégep, si le renseignement est nécessaire aux fins d'une procédure judiciaire autre qu'une procédure visée dans le paragraphe 1° ;

  3° À un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec ;

  4° À une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée.

- À l'article 59.1 ;

  En vue de prévenir un acte de violence, dont un suicide, lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable et que la nature de la menace inspire un sentiment d'urgence.

  Les renseignements peuvent alors être communiqués à la ou aux personnes exposées à ce danger, à leur représentant ou à toute personne susceptible de leur porter secours.

- À l'article 65.1 (1° à 3°) ;

  1° Lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli ;

  2° Lorsque son utilisation est manifestement au bénéfice de la personne concernée;

  3° Lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi.

- À l'article 66 ;

  Afin de recueillir des renseignements personnels déjà colligés par une personne ou un organisme privé.

- À l'article 67 ;

  À toute personne ou organisme si cette communication est nécessaire à l'application d'une loi au Québec, que cette communication soit ou non prévue expressément par la loi.

- À l'article 67.1 ;

  À toute personne ou organisme si cette communication est nécessaire à l'application d'une convention collective, d'un décret, d'un arrêté, d'une directive ou d'un règlement qui établissent des conditions de travail.

- À l'article 67.2 ;

  À toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise confié par l'organisme public à cette personne ou à cet organisme.

- À l'article 67.2.1 ;

  À une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques.

- À l'article 68

  1° À un organisme public ou à un organisme d'un autre gouvernement lorsque cette communication est nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en œuvre d'un programme dont cet organisme a la gestion ;

  1.1° À un organisme public ou à un organisme d'un autre gouvernement lorsque la communication est manifestement au bénéfice de la personne concernée ;

  2° À une personne ou à un organisme lorsque des circonstances exceptionnelles le justifient;

  3° À une personne ou à un organisme si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de l'identification de cette personne.

Ce registre de communication des renseignements personnels doit contenir les informations suivantes :

1. La nature ou le type de renseignement communiqué ;
2. La personne ou l'organisme qui reçoit cette communication ;
3. La fin pour laquelle ce renseignement est communiqué et l'indication, le cas échéant, qu'il s'agit d'une communication visée à l'article 70.1 ;
4. La raison justifiant cette communication.

Annexe C

EXEMPLES CONCRETS D'INCIDENTS DE CONFIDENTIALITÉ, NOTAMMENT :

- Un membre du personnel qui consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions en outrepassant les droits d'accès qui lui ont été consentis ou un pirate informatique qui s'infiltre dans un système ;
- Un membre du personnel qui utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne ;
- Une communication faite par erreur à la mauvaise personne par son employeur ;
- Une personne qui perd ou se fait voler des documents contenant des renseignements personnels ;
- Une personne qui s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer ;
- L'oubli de caviarder des renseignements personnels dans un document ;
- L'envoi d'un courriel contenant des renseignements personnels ;
- La communication d'un renseignement personnel contraire aux dispositions de la Loi sur l'accès ;
- Un membre du personnel consulte un renseignement personnel sans autorisation ;
- Un membre du personnel communique des renseignements personnels au mauvais destinataire ;
- L'organisation est victime d'une cyberattaque, comme de l'hameçonnage ou un rançongiciel.

Annexe D

REGISTRE D'INCIDENTS DE CONFIDENTIALITÉ

Voici un aide-mémoire indiquant les différentes étapes du traitement d'un incident de confidentialité :

AVIS À LA CAI	AVIS AUX PERSONNES CONCERNÉES	REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ
Le nom de l'organisation ayant fait l'objet de l'incident.	Description des renseignements personnels visés par l'incident ou la raison justifiant l'impossibilité de fournir une telle description.	Description des renseignements personnels visés par l'incident ou la raison justifiant l'impossibilité de fournir une telle description
Le nom et les coordonnées de la personne à contacter.	Brève description des circonstances de l'incident et, si elle est connue, la cause.	Brève description des circonstances de l'incident et, si elle est connue, la cause.
Description des renseignements personnels visés par l'incident ou la raison justifiant l'impossibilité de fournir une telle description.	La date ou la période où l'incident a eu lieu (ou approximation).	La date ou la période où l'incident a eu lieu (ou approximation)
Brève description des circonstances de l'incident et, si elle est connue, la cause.	La date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident.	Le nombre de personnes concernées par l'incident.
La date ou la période où l'incident a eu lieu (ou approximation).	Le nombre de personnes concernées par l'incident.	Description des éléments qui permettent de conclure qu'il existe un risque de préjudice
La date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident.	Description des éléments qui permettent de conclure qu'il existe un risque de préjudice.	Si l'incident présente un risque de préjudice sérieux, les dates de transmission des avis à la CAI et aux personnes concernées, accompagnées d'une mention indiquant si des avis publics ont été donnés par l'organisation et la raison.
Le nombre de personnes concernées par l'incident.	Les mesures prises par l'organisation ou celles qu'elle entend prendre afin d'aviser les personnes concernées (en vertu de l'article 63.8 de la Loi 25) ainsi que la date de l'avis, le cas échéant.	Brève description des mesures prises par l'organisation afin de diminuer les risques qu'un préjudice soit causé.
Description des éléments qui permettent de conclure qu'il existe un risque de préjudice.	Les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice.	**OBLIGATION DE TENIR LES RENSEIGNEMENTS AU REGISTRE À JOUR.**

AVIS À LA CAI	AVIS AUX PERSONNES CONCERNÉES	REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ
Les mesures prises par l'organisation ou celles qu'elle entend prendre afin d'aviser les personnes concernées (en vertu de l'article 63.8 de la Loi 25) ainsi que la date de l'avis, le cas échéant.	Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.	**OBLIGATION DE CONSERVATION PENDANT UNE PÉRIODE MINIMALE DE 5 ANS APRÈS LA DATE OU LA PÉRIODE AU COURS DE LAQUELLE L'ORGANISATION A PRIS CONNAISSANCE DE L'INCIDENT.**
Les mesures prises à la suite de l'incident.		
Une mention d'un avis envoyé auprès d'une autorité similaire à la CAI à l'extérieur du Québec.		
Tout renseignement ou information complémentaire suivant le dépôt d'un avis (souvent en annexe).		

EXEMPLE du registre d'incidents de confidentialité exigé par la Loi 25 :

Informations générales		
LE FORMULAIRE D'AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION PEUT ÊTRE CONSULTÉ ET TÉLÉCHARGÉ ICI : FORMULAIRE AVIS À LA CAI		
LES RENSEIGNEMENTS DANS CE REGISTRE DOIVENT ÊTRE TENUS À JOUR ET CONSERVÉS PENDANT UNE PÉRIODE MINIMALE DE 5 ANS APRÈS LA DATE OU LA PÉRIODE AU COURS DE LAQUELLE L'ORGANISATION A PRIS CONNAISSANCE DE L'INCIDENT		
INCIDENT NO.1		
DESCRIPTION DES RENSEIGNEMENTS PERSONNELS VISES PAR L'INCIDENT (**SECTION 4 – AVIS A LA CAI**)		
DESCRIPTION DES CIRCONSTANCES DE L'INCIDENT (**SECTION 3.1 – AVIS À LA CAI**)		
LA DATE OU LA PÉRIODE OÙ L'INCIDENT A EU LIEU (OU APPROXIMATION) (**SECTION 2 - AVIS À LA CAI**)		
LA DATE OU LA PÉRIODE AU COURS DE LAQUELLE L'ORGANISATION A PRIS CONNAISSANCE DE L'INCIDENT (**SECTION 2 -AVIS À LA CAI)**		
LE NOMBRE DE PERSONNES CONCERNÉES PAR L'INCIDENT (**SECTION 5 - AVIS À LA CAI**)		
DESCRIPTION DES ÉLÉMENTS QUI AMÈNENT L'ORGANISATION À CONCLURE QU'IL EXISTE OU NON UN RISQUE QU'UN PRÉJUDICE SOIT CAUSÉ AUX PERSONNES CONCERNÉES (**SECTION 6 - AVIS À LA CAI**)		
DATE DE L'AVIS À LA CAI (**SECTION 6 - AVIS À LA CAI)**		
DATE DE L'AVIS AUX PERSONNES CONCERNÉES (**SECTION 7 - AVIS À LA CAI**)		
ÉMISSION D'UN AVIS PUBLIC (**SECTION 7.2 - AVIS À LA CAI**)		
EST-CE QU'UN AVIS PUBLIC A ÉTÉ FAIT ?	Oui	Non
RAISONNEMENT POUR UN AVIS PUBLIC		
DESCRIPTION DES MESURES PRISES POUR DIMINUER LE RISQUE (**SECTION 8 - AVIS À LA CAI**)		
FIN DE L'ENTREE AU REGISTRE		

INCIDENT NO. 2		
DESCRIPTION DES RENSEIGNEMENTS PERSONNELS VISES PAR L'INCIDENT (**SECTION 4 – AVIS A LA CAI**)		
DESCRIPTION DES CIRCONSTANCES DE L'INCIDENT (**SECTION 3.1 – AVIS À LA CAI**)		
LA DATE OU LA PÉRIODE OÙ L'INCIDENT A EU LIEU (OU APPROXIMATION) (**SECTION 2 - AVIS À LA CAI**)		
LA DATE OU LA PÉRIODE AU COURS DE LAQUELLE L'ORGANISATION A PRIS CONNAISSANCE DE L'INCIDENT (**SECTION 2 -AVIS À LA CAI)**		
LE NOMBRE DE PERSONNES CONCERNÉES PAR L'INCIDENT (**SECTION 5 - AVIS À LA CAI**)		
DESCRIPTION DES ÉLÉMENTS QUI AMÈNENT L'ORGANISATION À CONCLURE QU'IL EXISTE OU NON UN RISQUE QU'UN PRÉJUDICE SOIT CAUSÉ AUX PERSONNES CONCERNÉES (**SECTION 6 - AVIS À LA CAI**)		
DATE DE L'AVIS À LA CAI (**SECTION 6 - AVIS À LA CAI)**		
DATE DE L'AVIS AUX PERSONNES CONCERNÉES (**SECTION 7 - AVIS À LA CAI**)		
ÉMISSION D'UN AVIS PUBLIC (**SECTION 7.2 - AVIS À LA CAI**)		
EST-CE QU'UN AVIS PUBLIC A ÉTÉ FAIT ?	Oui	Non
RAISONNEMENT POUR UN AVIS PUBLIC		
DESCRIPTION DES MESURES PRISES POUR DIMINUER LE RISQUE (**SECTION 8 - AVIS À LA CAI**)		
FIN DE L'ENTREE AU REGISTRE		

INCIDENT NO. ___		
DESCRIPTION DES RENSEIGNEMENTS PERSONNELS VISES PAR L'INCIDENT (**SECTION 4 – AVIS A LA CAI**)		
DESCRIPTION DES CIRCONSTANCES DE L'INCIDENT (**SECTION 3.1 – AVIS À LA CAI**)		
LA DATE OU LA PÉRIODE OÙ L'INCIDENT A EU LIEU (OU APPROXIMATION) (**SECTION 2 - AVIS À LA CAI**)		
LA DATE OU LA PÉRIODE AU COURS DE LAQUELLE L'ORGANISATION A PRIS CONNAISSANCE DE L'INCIDENT (**SECTION 2 -AVIS À LA CAI)**		
LE NOMBRE DE PERSONNES CONCERNÉES PAR L'INCIDENT (**SECTION 5 - AVIS À LA CAI**)		
DESCRIPTION DES ÉLÉMENTS QUI AMÈNENT L'ORGANISATION À CONCLURE QU'IL EXISTE OU NON UN RISQUE QU'UN PRÉJUDICE SOIT CAUSÉ AUX PERSONNES CONCERNÉES (**SECTION 6 - AVIS À LA CAI**)		
DATE DE L'AVIS À LA CAI (**SECTION 6 - AVIS À LA CAI)**		
DATE DE L'AVIS AUX PERSONNES CONCERNÉES (**SECTION 7 - AVIS À LA CAI**)		
ÉMISSION D'UN AVIS PUBLIC (**SECTION 7.2 - AVIS À LA CAI**)		
EST-CE QU'UN AVIS PUBLIC A ÉTÉ FAIT ?	Oui	Non
RAISONNEMENT POUR UN AVIS PUBLIC		
DESCRIPTION DES MESURES PRISES POUR DIMINUER LE RISQUE (**SECTION 8 - AVIS À LA CAI**)		
FIN DE L'ENTREE AU REGISTRE		

Références

Commission d'accès à l'information du Québec (CAI). *Évaluation des facteurs relatifs à la vie privée*, URL :https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/evaluation-facteurs-relatifs-vie-privee/

Commission d'accès à l'information du Québec (CAI). Formulaires et lettres types, *Pour les citoyens*, URL : https://www.cai.gouv.qc.ca/formulaires-et-lettres-types/pour-les-citoyens/

Cégep de Rivière-du-Loup, Secrétariat général (11 avril 2023). *Directive relative à l'application des règles de gouvernance en matière de protection des renseignements personnels*, URL : https://www.cegeprdl.ca/media/10907016/1126-05-25-directive-en-matie-re-de-prp-vf.pdf

Cégep de Saint-Jérôme, Secrétariat général et affaires juridiques (11 octobre 2022). *Directive du comité de l'accès à l'information et de la protection des renseignements personnels (CAIPRP)*, URL : https://cdn.cstj.qc.ca/wp-content/uploads/2022/10/27154358/Directive_CAIPRP.pdf

Cégep de Valleyfield (2010). *Politique de service à la clientèle et de gestion des plaintes*, URL : https://www.cegepvalleyfield.ca/wp-content/uploads/2023/04/ag-10-po-08_service-clientele-et-gestion-plaintes-originale-9-fevrier-2010.pdf

Gouvernement du Québec (2022). *Comité sur l'accès à l'information et la protection des renseignements personnels,* URL : Comité sur l'accès à l'information et la protection des renseignements personnels (quebec.ca)

Gouvernement du Québec (2023). *Définitions de mots en lien avec la protection des renseignements personnels*, URL : https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/definitions-concepts/lexique

Fédération des cégeps (2023). *Guide concernant la protection des renseignements personnels et le partage d'informations au collégial*, URL : https://fedecegeps.ca/wp-content/uploads/2023/05/2023-03-17-daj-guide-protection-renseignements-personnels-et-partage-info-au-collegial.pdf

Norme ISO 31700-1 :2023. *Protection des consommateurs – Respect de la vie privée assuré dès la conception des biens de consommation et services aux consommateurs*, URL : https://www.iso.org/fr/standard/84977.html

Publications Québec (2023). *Charte des droits et libertés de la personne* (RLRQ, c. C-12), URL : https://www.legisquebec.gouv.qc.ca/fr/document/lc/C-12

Publications Québec (2023). *Code civil du Québec*, (RLRQ, c. CCQ-1991).
URL : https://www.legisquebec.gouv.qc.ca/fr/document/lc/CCQ-1991

Publications Québec (2023). *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1), URL : https://www.legisquebec.gouv.qc.ca/fr/document/lc/A-2.1

Publications Québec (2021). *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (L.Q. 2021, c. 25), URL : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2021/2021C25F.PDF