



Stratégie institutionnelle de gestion des données de la recherche

Collège Laflèche

*« Un milieu de travail où la recherche et le
développement pédagogique sont possibles et valorisés. »*

Orientation 4 : « Mettre en place une culture d'innovation et les ressources nécessaires. »

Plan stratégique 2022-2027, Collège Laflèche

Adopté à la rencontre du
Comité de direction du 24 avril 2023

Table des matières

1.	Préambule	03
2.	Objectif	04
3.	Obligations et principes directeurs	04
	3.1 Obligation pour le Collège	04
	3.2 Obligations pour les chercheurs et les chercheuses	05
	3.3 Principes FAIR	05
	3.4 Principes PCAP	06
4.	Composantes et stratégie	07
	4.1 La sensibilisation de la communauté	07
	4.2 La formalisation	08
	4.3 La formation	08
	4.4 L'évaluation continue	09
5.	État des lieux et actions à mener	10
6.	Tableau de mise en œuvre	19
7.	Annexe 1 : Quelques définitions	24
8.	Bibliographie	34

1. Préambule

Le Collège Laflèche promeut, favorise et soutient la recherche et son déploiement depuis maintenant plus d'une décennie. En effet, c'est en septembre 2012 que le Collège Laflèche adoptait, par son Conseil d'administration, les premières politiques institutionnelles au sujet de la recherche¹. Depuis, elles ont été successivement bonifiées au fil des années et des attentes de la part des différents organismes subventionnaires, fédéraux comme provinciaux. Pour le Collège Laflèche, il est évident que la recherche et sa diversité a un effet positif sur l'ensemble des personnes qui constitue sa communauté de même que sur la qualité du perfectionnement des professeurs et professeures ainsi que sur la qualité de l'enseignement.

En 2018, l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) publie une importante recommandation² concernant la science et les chercheurs scientifiques dans laquelle est proposé aux états membres les modalités d'élaboration d'une politique nationale de la recherche. Les conditions de la recherche, de son financement, de l'éducation et de la formation initiales de ses chercheurs comme de ses chercheuses, les droits et responsabilités qui incombent aux parties prenantes dans le domaine de la recherche et les conditions de leur réussite structurent la recommandation de l'organisme. La présente stratégie s'inscrit dans cette volonté de mettre en œuvre l'ensemble des conditions pour que la recherche scientifique puisse progresser, grandir et orienter les communautés. Pour y arriver, l'UNESCO suggère aux états membres, entre autres, d'« assurer un accès libre et équitable à la littérature, aux données et aux contenus scientifiques, notamment en supprimant les obstacles à la publication, au partage et à l'archivage des résultats scientifiques. »³

C'est dans cette perspective que les trois organismes fédéraux⁴ se sont dotés d'une politique⁵ afin d'encadrer les conditions de publication, partage et d'archivage des données de recherche scientifique. L'objectif de la *Politique* est de « promouvoir l'excellence en matière de recherche au Canada en encourageant de saines pratiques de gestion des données de recherche et d'intendance de données. »⁶ Les trois organismes conviennent que « la capacité de stocker, de consulter, de réutiliser et de mettre à profit les données numériques de la recherche est devenue essentielle à l'avancement de la science (...) et que les données recueillies par la recherche grâce

¹ Il s'agissait de la *Politique institutionnelle de la recherche*, de la *Politique institutionnelle d'éthique de la recherche avec des êtres humains*, de la *Politique institutionnelle sur la conduite responsable en recherche* et de sa *Politique institutionnelle sur les conflits d'intérêts en recherche*.

² UNESCO, (2018). *Recommandation concernant la science et les chercheurs scientifiques*.

³ UNESCO, (2018). *Recommandation concernant la science et les chercheurs scientifiques, 13 e*, p. 11.

⁴ Il s'agit du Conseil de recherches en sciences humaines du Canada (CRSH), du Conseil de recherches en sciences naturelles et en génie (CRSNG) et les Instituts de recherche en santé du Canada (IRSC).

⁵ CRSH, CRSNG et IRSC. (2022). *Politique des trois organismes sur la gestion des données de recherche*.

⁶ CRSH, CRSNG et IRSC. (2022). *Politique des trois organismes sur la gestion des données de recherche*. Par ailleurs, elle spécifie « que la politique n'est pas une politique sur les données ouvertes. » pt. 2, p. 3-4.

aux fonds publics doivent être gérées de manière responsable et efficaces et qu'elles appartiennent, dans la mesure du possible, au domaine public. »

Les trois Fonds de recherche du Québec poursuivront essentiellement le même objectif de diffusion favorisant un accès équitable aux données et aux résultats de la recherche scientifique financée.⁷

Ainsi, la présente stratégie suivra les prescriptions et la mise en œuvre proposées par les organismes subventionnaires et fera l'objet d'une révision par les membres de la direction ainsi que les membres du Comité d'éthique de la recherche avec des êtres humains du Collège Laflèche. Elle sera présentée aux organismes subventionnaires fédéraux et provinciaux avec lesquels nous avons une reconnaissance et une entente d'admissibilité complète à titre d'établissement d'enseignement supérieur gestionnaire de fonds de recherche.

2. Objectif

Le Collège reconnaît l'importance de bien gérer les données de recherche et d'y donner accès, à la fois pour vérification et la transparence de la recherche ainsi que pour la réutilisation et l'intégration des données au profit de nouvelles recherches et de nouveaux résultats. De cette manière, la présente *Stratégie* permettra de développer une vision commune et des pratiques responsables en matière de gestion des données de la recherche.

3. Obligations et principes directeurs

3.1 Obligation pour le Collège :

- a) Le Collège Laflèche est un établissement d'enseignement supérieur bénéficiant d'une pleine reconnaissance et d'une entière admissibilité à administrer des fonds des organismes fédéraux (CRSH et CRSNG) et des Fonds de recherche du Québec. Dans cette perspective, il se dote d'une stratégie de gestion des données de recherche en conformité avec l'exigence des organismes subventionnaires fédéraux. La mise en œuvre de cette stratégie permettra, éventuellement, de se doter d'une Politique institutionnelle de la gestion des données de recherche.

⁷ Il s'agit des Fonds de recherche du Québec - société et culture (FRQSC), Nature et technologie (FRQNT) et Santé (FRQS).

- b) Le Collège reconnaît l'importance d'une saine pratique de gestion des données de gestion ainsi que leur intendance. Dans cette perspective, le Collège s'engage à déployer les moyens et les processus afin de soutenir ses chercheurs et chercheuses dans l'élaboration de leur plan de gestion des données de recherche.

3.2 **Obligations pour les chercheurs et les chercheuses :**

- a) Toutes les demandes de subvention doivent inclure des méthodologies qui tiennent compte des meilleures pratiques en matière de gestion des données de recherche. Dans certaines occasions de financement, les organismes subventionnaires exigeront des chercheurs et des chercheuses qu'un plan de gestion des données de recherche (PGD) soit soumis avec certaines demandes de financement. Dans ces cas, les PGD seront examinés dans le processus de prise de décision.
- b) Les titulaires de subvention seront tenus de verser dans un dépôt numérique qui assure le stockage, la conservation et la curation sécuritaires des données de recherche.
- c) Les titulaires de subvention ne sont pas tenus de partager leurs données, mais les organismes subventionnaires s'attendent à ce que les chercheurs et les chercheuses donnent un accès convenable conformément aux principes FAIR⁸ ainsi qu'aux principes PCAP et aux normes propres aux disciplines, pour autant que les exigences éthiques, culturelles, juridiques et commerciales le permettent.

3.3 Les principes FAIR⁹ : Les données téléversées dans des dépôts doivent répondre aux principes FAIR, un acronyme formé à partir des quatre mots anglais suivants :

- a) *Findable* (facile à trouver) :

Les données doivent être décrites au moyen de métadonnées représentatives des données de recherche du regroupement. Elles doivent idéalement avoir un identifiant permanent unique tel un DOI (Digital Object Identifier), qui est déterminé selon une méthode standardisée pour identifier des objets électroniques de façon permanente.

⁸ Les principes FAIR et PCAP seront présentés à la suite des obligations.

⁹ Voir Wilkinson, M. D., Dumontier, M., Aalbersberg, Lj. J., Appleton, G., Axton, M., Baak, A., ... Mons, B. (2016). *The Fair Guiding Principles for Scientific data management and stewardship*. Scientific Data, 3 160018. <https://www.nature.com/articles/sdata201618> Voir aussi, Alliance de recherche numérique du Canada à l'adresse électronique suivante : info@alliancecan.ca ou portage@carl-abrc.ca

b) **Accessible** (accessible) :

Les données peuvent être facilement obtenues à l'aide de moteurs de recherche utilisant des protocoles définis et standardisés, et les conditions d'accès aux données doivent être clairement établies.

c) **Interoperables** (interopérable) :

L'interopérabilité est la capacité que possède un système informatique à fonctionner avec d'autres produits ou systèmes informatiques sans restriction d'accès ou de mise en œuvre.

d) **Reusable** (réutilisable) :

Les formats de données et de métadonnées sont optimisés pour favoriser la réutilisation. Les fichiers doivent donc être clairement détaillés et les informations nécessaires à la réutilisation des données doivent y figurer.

3.4 Les principes PCAP¹⁰ : Selon les principes PCAP (propriété, contrôle, accès et possession), les Premières Nations contrôlent les processus de collecte de données dans leurs communautés. Les Premières Nations sont propriétaires des renseignements les concernant et décident sur le bien-fondé de leur protection et de leur utilisation. Il est important d'assurer l'accès aux données sur les Premières Nations, mais ce sont les Premières Nations qui, en vertu de mandats et de protocoles appropriés, facilitent et règlementent cet accès. Les droits des communautés des Premières Nations d'être propriétaires des renseignements les concernant, de les contrôler et d'y avoir accès sont étroitement liés à leur autodétermination ainsi qu'à la préservation et au développement de leur culture. Grâce aux principes PCAP, les communautés peuvent déterminer les diverses étapes de la collecte des données, c'est-à-dire l'objectif principal, les moyens employés et les personnes responsables de la collecte, ainsi que décider de l'utilisation et de la communication de ces renseignements.

a) **Propriété** :

Il s'agit de la relation que les Premières Nations entretiennent avec leur savoir culturel et leurs données et renseignements les concernant. Selon ce principe, une communauté ou un groupe est collectivement propriétaire de l'information, à l'instar d'un individu qui est naturellement propriétaire de ses renseignements personnels.

¹⁰ Voir <http://www.fnigc.ca/fr/pcap.html>

b) **Contrôle** :

Selon ce principe, les Premières Nations, leurs communautés et les organismes qui les représentent ont le droit d'exiger le contrôle d'intégralité de la recherche et des processus de gestion de l'information les concernant. Le contrôle de la recherche peut comprendre toutes les étapes d'un projet, c'est-à-dire du début à la fin. Le principe concerne aussi le contrôle de divers processus, dont l'attribution des ressources et l'examen, la planification, la gestion de l'information.

c) **Accès** :

Quel que soit l'endroit où se trouvent des renseignements et données concernant les Premières Nations et leurs communautés, les Premières Nations doivent y avoir accès. Ce principe confirme également le droit des communautés et des organisations des Premières Nations de prendre des décisions concernant l'accès à leur information collective et la gestion de cet accès. Concrètement, ce droit peut être exercé au moyen de protocoles officiels normalisés.

d) **Possession** :

Alors que la propriété définit la relation qui existe entre un peuple et l'information le concernant, la possession ou la gestion est, quant à elle, un principe plus concret. Il s'agit du contrôle matériel des données. La possession est un mécanisme permettant de faire valoir et de protéger la propriété.

4. Composantes et stratégie

Le Collège Laflèche reconnaît l'importance des données de recherche. En effet, elles représentent non seulement des éléments déterminants du processus de la démarche scientifique mais aussi, elles rendent possibles la création de nouvelles connaissances. Elles peuvent très bien être la source de nouvelles recherches. Dans cette perspective, elles doivent être gérées efficacement afin de les protéger tout en les rendant accessibles.

Les composantes de la stratégie de gestion des données de recherche

4.1 La sensibilisation de la communauté

Le Collège veut développer une culture de science ouverte par le partage et la réutilisation des données de recherche, que celles-ci soient produites par

les membres de sa communauté ou par les collaboratrices et les collaborateurs externes de ses chercheuses et de ses chercheurs. Il souhaite également que ses étudiantes et ses étudiants connaissent et utilisent les données de recherche qui sont diffusées dans des dépôts numériques pour réaliser des travaux dans le cadre de leurs cours.

4.2 La formalisation

La gestion des données de recherche est pratiquée à tous les stades d'un projet de recherche, depuis sa planification jusqu'à la diffusion des résultats. L'outil de base de la GDR est le plan de gestion des données de recherche (PGD). Celui-ci est basé sur un ensemble de bonnes pratiques simples que l'ensemble des chercheuses et des chercheurs peuvent adopter, peu importe leurs compétences et leur niveau d'expertise en la matière. Le Collège diffusera la boîte à outil (Guide) développée par le réseau Portage¹¹ auprès des chercheuses et des chercheurs du Collège.

4.3 La formation

Le Collège reconnaît l'importance que le personnel impliqué dans la gestion des données de recherche soit constamment informé des nouveautés au sujet des pratiques de gestion des données de recherche. Il sera responsable du transfert de l'information et de l'expertise auprès des chercheuses et des chercheurs comme des étudiantes et des étudiants qui font de l'initiation à la recherche.

Dans cette perspective, les chercheuses et les chercheurs comme les étudiantes et les étudiants qui font ou s'initient à la recherche recevront des formations relatives à la gestion des données de la recherche. Ces formations pourront être données par des personnes intervenantes provenant tant de l'interne que de l'externe. Il peut également s'agir d'activité de formation en ligne réalisées de façon autonome.

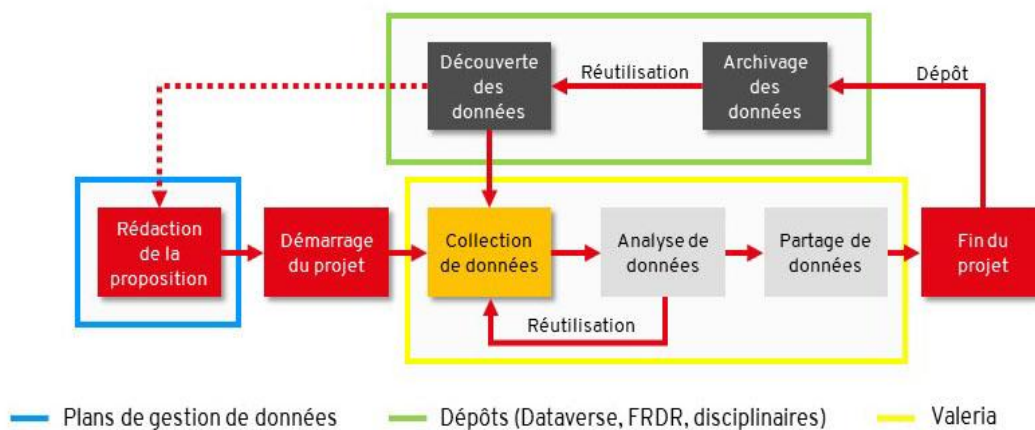
Le Collège participe activement aux activités des communautés de pratique en gestion des données de recherche du milieu collégial comme de tout ce qui concerne, de près et de loin à la recherche au niveau collégial. Celles de l'ARC, celles de l'Association pour les collèges privés du Québec (ACPQ) et celles du ministère de l'Enseignement supérieur (MES).

¹¹ Le réseau Portage est un organisme qui a été intégré à Alliance numérique du Canada. Dans la même perspective, l'Association pour la recherche au Collégial (ARC) développe actuellement des outils à cet effet et compte mettre sur pied une communauté de pratique au sujet de la gestion des données de recherche. Le Collège y participera puisqu'il est membre corporatif de l'ARC.

4.4 La formation continue

Le Collège évalue l'ensemble des pratiques concernant la recherche sur une base régulière afin d'y apporter des correctifs et/ou des modifications pour rendre ses Politiques institutionnelles et sa stratégie les plus efficaces et, lorsque cela est nécessaire, de les mettre à jour.

Le cycle de vie des données de recherche au Collège est le suivant¹² :



¹² Voir University of Virginia Library cite par Université Laval, (2022). *Stratégie institutionnelle pour la gestion des données de recherche*.

5. État des lieux et actions à mener

Cette section présente les objectifs et l'état des lieux concernant les aspects institutionnels de la gestion des données de recherche du Collège Laflèche. Par la suite, le même exercice sera mené pour les quatre composantes de notre stratégie de gestion des données de recherche, c'est-à-dire la sensibilisation, la formalisation, la formation et l'évaluation continue.

5.1 Considérations institutionnelles

5.1.1 Infrastructure et ressources en matière de technologie de l'information

Éléments	État actuelle de la situation	Action(s) à faire	Échéancier et responsables
Infrastructure et services connexes couvrant la gestion et la vérification de l'identité.	<p>Tous les compte Microsoft 365 du Collège sont hautement sécurisés par des processus de vérification de l'identité.</p> <p>Les mots de passe doivent être régulièrement changés.</p> <p>Des sauvegardes du contenu de l'Intranet sont réalisées quotidiennement et des copies sont faites sur les serveurs du Collège et sur des serveurs externes.</p>	<p><u>Créer une bibliothèque Teams</u> pour les données de recherche y incluant pour les projets passés disponibles.</p> <p>En continuité avec les processus déjà en place au Collège, chaque projet de recherche se verra attribuer un espace de travail collaboratif Microsoft 365 (espace de travail et stockage).</p> <p>S'assurer que les personnes qui font de la recherche au Collège</p> <p>a) Transfèrent toutes leurs données de recherche dans la bibliothèque ; b) Qu'elles détruisent toutes les copies de leurs données qui ont été sauvegardées sur d'autres médias ; c) Qu'elles utilisent uniquement ce</p>	<p>Hiver 2023</p> <p>Directeur adjoint - Ressources informationnelles</p> <p>Automne 2023 (En continu)</p> <p>Directeur adjoint - Ressources informationnelles</p> <p>Automne 2023 (En continu)</p> <p>Déploiement de la recherche</p>

		moyen de conservation l'avenir.	
Accès médiatisé aux données de recherche en fonction des besoins de sécurité.	Aucun accès aux données de recherche actuellement autre que les chercheurs et chercheuses pour leur projet de recherche.	<p><u>Créer les modalités d'accès et les conditions d'accès aux données de recherche.</u></p> <p>En cours de projet, seuls les membres de l'équipe du projet de recherche auront accès aux données.</p> <p>Le chercheur ou la chercheuse principale et le gérant de la bibliothèque gèrent les autorisations d'accès et élaborent les <u>protocoles d'utilisation des données de recherche.</u></p>	<p>Automne 2023</p> <p>Directeur adjoint - Ressources informationnelles</p> <p>Directeur adjoint - Ressources informationnelles et les chercheurs-chercheuses</p> <p>Automne 2023 – Hiver 2024</p>
Espace de stockage actif.	Le Collège dispose de 1300Tb d'espace de stockage et celui-ci est actuellement utilisé à peine à 4% de sa capacité. Il ne semble pas y avoir, à court et moyen terme, d'enjeu concernant le stockage des données dans une bibliothèque virtuelle.	Aucune	<p>Dès maintenant</p> <p>Directeur adjoint - Ressources informationnelles</p>
Espace de stockage sécurisé et géré par l'établissement pour les projets actifs qui comportent des données sensibles ou confidentielles.	L'espace de stockage actif ci-dessus est utilisé pour les données sensibles. Les personnes qui y ont accès sont le gérant des données ou la personne chargée de gérer les accès et les personnes responsables des projets de recherche.	Aucune	<p>Dès maintenant</p> <p>Directeur adjoint - Ressources informationnelles</p>
Espace de stockage pour préservation et les archives.	Le Collège ne dispose pas encore d'espace de stockage	Les données de recherche seront transférées dans <u>notre</u>	Hiver 2024

	numérique pour ses archives.	<u>système d'archivage numérique (SYGED)</u> seront accessibles, en consultation seulement, selon les critères établis par les responsables du projet de recherche en question.	Directeur adjoint - Ressources informationnelles
Dépôt pour la consignation et la diffusion des données de recherche.	Le Collège ne dispose pas de plateforme de diffusion des données pour l'instant.	<u>Une étude devra être faite</u> concernant les plateformes de consignation et de diffusion des données existantes. <u>Évaluer la possibilité de mutualiser</u> une plateforme de consignation et de diffusion des données au sein de l'Association des collèges privés du Québec.	Automne 2023 Directeur adjoint - Ressources informationnelles 2023 – 2024 Directeur adjoint - Ressources informationnelles et Déploiement de la recherche
Inventaire des données de recherche au Collège	A venir	<u>Une étude est en cours</u> au Collège.	En cours Directeur adjoint - Ressources informationnelles

5.1.2 Les politiques, les procédures et les règlements

Éléments	État actuelle de la situation	Action(s) à faire	Échéancier et responsables
Politique institutionnelle de gestion des données de recherche	Actuellement, la <i>Politique institutionnelle sur la conduite responsable en recherche</i> du Collège donne des lignes directrices sur la conservation des données de recherche.	À la suite de notre <i>Stratégie institutionnelles de gestion des données de recherche</i> , nous <u>rédigerons une <i>Politique institutionnelle de la gestion des données</i></u>	Automne 2023 Déploiement de la recherche

		<i>de recherche</i> qui balisera les quatre composantes de notre stratégie et répartira les responsabilités aux différentes parties prenantes.	
Politique de sécurité des ressources technologiques.	La politique est en place et disponible sur l'intranet du Collège.	<u>Bonifier la politique</u> afin de préserver la confidentialité des données de recherche durant toutes les étapes de son cycle de vie.	2023 – 2024 Directeur adjoint - Ressources informationnelles
Procédures de sécurité et d'évaluation des risques.	Un projet de politique d'évaluation des risques est en cours.	<u>Rédiger une politique sur l'évaluation des risques et la sécurité</u> en ce qui concerne les questions juridiques, la vulnérabilité et la confidentialité qui inclurait les données de recherche.	2023 – 2024 Directrice - Services administratifs

5.1.3 Les ressources humaines

Éléments	État actuelle de la situation	Action(s) à faire	Échéancier et responsables
Personne responsable de la protection des données.	Le directeur adjoint aux ressources informationnelles ou le gérant des données, assure cette responsabilité.	Formation d'un comité de gestion des données de recherche au Collège.	Automne 2023 Direction des études, Directeur adjoint - Ressources informationnelles et Déploiement de la recherche

5.2 Les composantes de notre stratégie de gestion des données de recherche

5.2.1 Sensibilisation à la gestion des données de recherche

Éléments	État actuelle de la situation	Action(s) à faire	Échéancier et responsables
<p>Plan de promotion de la gestion des données de recherche.</p>	<p>La direction générale et la direction des études connaissent les enjeux liés à la gestion des données de recherche.</p> <p>La direction adjointe aux ressources informationnelles connaît les enjeux liés à la gestion des données de recherche.</p>	<p><u>Élaborer un plan de promotion</u> de la gestion des données de recherche et le diffuser auprès des chercheuses et des chercheurs du Collège.</p> <p><u>Informer tous les membres de la direction</u> du Collège Laflèche de la Politique des trois organismes sur la gestion des données de recherche.</p> <p><u>Sensibiliser la communauté du Collège Laflèche</u> à la gestion des données de recherche, faire connaître les politiques des organismes subventionnaires, les politiques institutionnelles concernant la recherche ainsi que la stratégie institutionnelle de la gestion des données de la recherche du Collège.</p>	<p>Hiver 2024</p> <p>Responsable des communications, des affaires institutionnelles et de l'International et Déploiement de la recherche</p> <p>Automne 2023 Hiver 2024</p> <p>Direction des études et Déploiement de la recherche</p>

Diffusion sur internet	Aucune pour le moment.	<u>Créer une page web</u> afin de décrire les principes de base de la gestion des données de recherche. En assurer la mise à jour.	Hiver 2024 Responsable des communications, des affaires institutionnelles et de l'International
Recherche par et avec des membres des Premières Nations.	Actuellement, aucune chercheuse et aucun chercheur du Collège ne réalise des travaux de recherche avec des membres des communautés des Premières Nations.	Faire en sorte que toutes les parties prenantes comprennent les enjeux reliés à la recherche avec des membres des Premières Nations. Soutenir adéquatement les personnes issues de ses communauté ou toute personne qui entreprendra un projet de recherche avec des membres de la communauté des Premières Nations.	2023 – 2024 Déploiement de la recherche 2023 – 2024 Déploiement de la recherche

5.2.2 Formalisation de la gestion des données de recherche

Éléments	État actuelle de la situation	Action(s) à faire	Échéancier et responsables
Consultation générale concernant la gestion des données de recherche.	Aucune	<u>Une séance d'information</u> sur la gestion des données de recherche doit être faite. <u>Faire des consultations individuelles ou en groupes restreints</u> pour s'assurer de répondre à tous les besoins et à toutes les préoccupations.	Automne 2023 Déploiement de la recherche Hiver 2024 Déploiement de la recherche

Préparation d'un plan de gestion des données de recherche.	Aucun	<p><u>Produire un modèle de plan de gestion des données de recherche</u> au Collège influencé par les modèles de gestion des données de recherche produit par le groupe de travail sur les GDR de l'Association pour la recherche au Collégial (ARC). Le Collège est un membre actif de l'ARC.</p> <p><u>Diffuser le modèle de PGD</u> auprès des chercheuses et des chercheurs du Collège.</p>	<p>Automne 2023 – Hiver 2024</p> <p>Déploiement de la recherche</p> <p>Hiver 2024</p> <p>Déploiement de la recherche</p>
Gestion des risques	Le Collège ne dispose d'aucun outil à cet effet qui pourrait guider les chercheuses et les chercheurs du Collège.	<u>Créer un outil d'évaluation et de gestion des données de recherche</u> et le mettre à la disposition des chercheuses et des chercheurs.	<p>Automne 2024</p> <p>Déploiement de la recherche</p>
Préparation des données	Le Collège ne dispose d'aucun outil à cet effet qui pourrait guider les chercheuses et les chercheurs du Collège.	<p><u>Rechercher des outils appropriés concernant l'organisation et la préparation des données.</u></p> <p><u>Implantation de la plateforme SIGED Mobile.</u></p>	<p>Automne 2023</p> <p>Directeur adjoint - Ressources informationnelles et Déploiement de la recherche</p> <p>Hiver 2024</p> <p>Directeur adjoint - Ressources informationnelles</p>
Préparation des métadonnées.	Le Collège dispose d'un système de gestion numérique des archives. Il permet de préciser les métadonnées reliées à un document et dresse également, de façon automatique, une liste des termes clés de	<u>Implantation de la plateforme SIGED Mobile.</u>	<p>Hiver 2024</p> <p>Directeur adjoint - Ressources informationnelles</p>

	chacun des documents. Il permet aussi une recherche plein texte.		
Identification de dépôts de données.	Nous sommes en cours d'identification.	<p><u>Explorer les dépôts à lesquels nous pourrions nous joindre ou se doter d'un dépôt de données accessible et répondant aux besoins des chercheuses et des chercheurs du Collège.</u></p> <p>Dans cette perspective, <u>explorer la possibilité de développer ou s'associer à un dépôt des données existant avec l'Association des collèges privés du Québec (ACPO) et ainsi mutualiser un dépôt pour tous les collèges privés québécois.</u></p>	<p>Automne 2024</p> <p>Directeur adjoint - Ressources informationnelles</p> <p>Automne 2024</p> <p>Directeur adjoint - Ressources informationnelles et Déploiement de la recherche</p>
Éthique de la recherche avec des êtres humains	Le Comité d'éthique de la recherche avec des êtres humains du Collège (CÉR) participera à la version finale de la Stratégie de gestion des données de recherche ainsi qu'à la Politique institutionnelle qui en découlera.	Que le CÉR puisse <u>soutenir les chercheuses et les chercheurs dans la gestion des données de recherche avec des êtres humains.</u>	<p>Automne 2023 (En continu)</p> <p>Déploiement de la recherche</p>

5.2.3 Formation à la gestion des données de recherche

Éléments	État actuelle de la situation	Action(s) à faire	Échéancier et responsables
Formation générale sur la gestion des données de recherche.	Tout est à faire	<p><u>Préparer et offrir une séance d'information afin de présenter la Politique de gestion des données de recherche des Trois organismes fédéraux.</u></p> <p><u>Préparer et offrir une rencontre d'information générale afin de présenter les processus institutionnels de gestion des données de recherche.</u></p> <p><u>Rédiger et publier un document qui résume les processus formels de gestion des données de recherche.</u></p> <p>S'inspirer des outils de gestion des données de recherche de l'Alliance numérique du Canada et des boîtes à outil de l'organisme Portage.</p>	<p>Automne 2023</p> <p>Déploiement de la recherche</p> <p>Hiver 2024</p> <p>Déploiement de la recherche</p> <p>Hiver 2024</p> <p>Déploiement de la recherche</p>
Formation sur la production d'un plan de gestion de données de recherche.	À faire	<p><u>Préparer et offrir une séance de formation sur la création de plan de gestion des données de recherche pour les chercheuses et les chercheurs du Collège.</u></p>	<p>Hiver 2024</p> <p>Déploiement de la recherche</p>
Formation sur la préparation des données et des métadonnées pour la diffusion dans un dépôt numérique.	À faire	<p><u>Préparer et offrir une formation sur la préparation de données et de métadonnées de recherche.</u></p>	<p>Automne 2024</p> <p>Déploiement de la recherche</p>

5.2.4 Évaluation continue de la stratégie de la gestion des données de recherche

Éléments	État actuelle de la situation	Action(s) à faire	Échéancier
Évaluation continue des pratiques en matière de recherche au Collège.	Toutes les politiques institutionnelles sont revues et bonifiées périodiquement.	<u>Prévoir une séquence d'évaluation dans la Politique</u> à venir afin d'assurer les normes de bonne gestion des données de la recherche au Collège.	Automne 2023 Déploiement de la recherche

- Directeur des études
- Directrice - Services administratifs
- Directeur adjoint - Ressources informationnelles
- Responsable des communications, des affaires institutionnelles et de l'International
- Déploiement de la recherche

6. Tableau de mise en œuvre

	Hiver 2023	Automne 2023	Hiver 2024	Automne 2024	Hiver 2025
Actions à faire	<ul style="list-style-type: none"> - Créer une bibliothèque Teams. - Une étude est en cours concernant l'inventaire des données de recherche au Collège. 	<ul style="list-style-type: none"> - S'assurer que les personnes qui font de la recherche au Collège <ol style="list-style-type: none"> a. Transfèrent toutes leurs données de recherche dans la bibliothèque ; b. Qu'elles détruisent toutes les copies de 		<ul style="list-style-type: none"> - Créer un outil d'évaluation et de gestion des données de recherche et le mettre à la disposition des chercheuses et des chercheurs. 	

Actions à faire		<p>leurs données qui ont été sauvegardées sur d'autres médias ;</p> <p>c. Quelles utilisent uniquement ce moyen de conservation l'avenir.</p>			
	- Espace de stockage actif.	- Créer les modalités d'accès et les conditions d'accès aux données de recherche.	- Implantation de la plateforme SIGED Mobile	- Explorer les dépôts à lesquels nous pourrions nous joindre ou se doter d'un dépôt de données.	
	- Espace de stockage sécurisé.	- Élaborent les protocoles d'utilisation des données de recherche.	- Transférer les données de recherche dans notre système d'archivage numérique (SYGED).	- Explorer la possibilité de développer ou s'associer à un dépôt des données existant avec l'Association des collèges privés du Québec (ACPQ) et ainsi mutualiser un dépôt pour tous les collèges privés québécois.	
	- Inventaire des données de recherche au Collège.	- Une étude devra être faite concernant les plateformes de consignation et de diffusion des données existantes.	- Évaluer la possibilité de mutualiser une plateforme de consignation et de diffusion des données au sein de l'Association des collèges privés du Québec.		

Actions à faire	- Une étude est en cours.	- Rédaction d'une Politique institutionnelle de la gestion des données de recherche.	- Bonifier la <i>Politique de sécurité des ressources technologiques</i> afin de préserver la confidentialité des données de recherche durant toutes les étapes de son cycle de vie.		
	- Que le CÉR puisse soutenir les chercheuses et les chercheurs dans la gestion des données de recherche avec des êtres humains. (En continu)	- Formation d'un comité de gestion des données de recherche au Collège.	- Rédiger une politique sur l'évaluation des risques et la sécurité en ce qui concerne les questions juridiques, la vulnérabilité et la confidentialité qui inclurait les données de recherche.		
		- Informer tous les membres de la direction du Collège Laflèche de la Politique des trois organismes sur la gestion des données de recherche.	- Élaborer un plan de promotion de la gestion des données de recherche et le diffuser auprès des chercheuses et des chercheurs du Collège.		
		- Faire en sorte que toutes les parties prenantes comprennent les enjeux liés à la recherche avec des membres des Premières Nations.	- Sensibiliser la communauté du Collège Laflèche à la gestion des données de recherche, faire connaître les politiques des organismes subventionnaires, les politiques institutionnelles concernant la		

Actions à faire		Soutenir adéquatement les personnes issues de ses communauté ou toute personne qui entreprendra un projet de recherche avec des membres de la communauté des Premières Nations.	recherche ainsi que la stratégie institutionnelle de la gestion des données de la recherche du Collège.		
		- Une séance de consultation générale sur la gestion des données de recherche doit être faite.	- Créer une page web afin de décrire les principes de base de la gestion des données de recherche.		
		- Rechercher des outils appropriés concernant l'organisation et la préparation des données.	- Faire des consultations individuelles ou en groupes restreints pour s'assurer de répondre à tous les besoins et à toutes les préoccupations. - Produire un modèle de plan de gestion des données de recherche au Collège.		
		- Préparer et offrir une séance d'information afin de présenter la Politique de gestion des données de recherche des Trois organismes fédéraux.	- Diffuser le modèle de PGD auprès des chercheuses et des chercheurs du Collège.		

Actions à faire		- Prévoir une séquence d'évaluation dans la Politique.	- Préparer et offrir une rencontre d'information générale afin de présenter les processus institutionnels de gestion des données de recherche.		
			- Préparer et offrir une séance de formation sur la création de plan de gestion des données de recherche pour les chercheuses et les chercheurs du Collège.		
			- Préparer et offrir une formation sur la préparation de données et de métadonnées de recherche.		

7. Annexe 1 : Quelques définitions

Les définitions que nous utilisons sont toutes tirées de la *Boîte à outils pour les données sensibles destiné aux chercheurs - Glossaire terminologique sur l'utilisation des données sensibles à des fins de recherche*¹³ préparé par le groupe d'experts sur les données sensibles (GEDS) du réseau Portage au nom de l'Association des bibliothèques de recherche du Canada (ABRC). Elles sont présentées en ordre alphabétique.

Accès aux données : Le droit ou la possibilité d'utiliser ou de consulter les données conservées dans une base de données ou un dépôt / un environnement de recherche / un environnement virtuel de recherche.

Autoriser l'accès aux données : Les chercheur ou la chercheuse autorise le personnel (à titre individuel ou fonctionnel) à accéder aux données.

Chiffrement : Processus de transformation de l'information en un format différent ou de cryptage des données.

Connaissances traditionnelles / données sur les spécificités autochtones : Connaissances (savoirs) détenues par les peuples des Premières Nations, les Inuits et les Métis, qui constituent les peuples autochtones du Canada. Ces connaissances se rattachent à un lieu précis, sont généralement transmises oralement et sont fondées sur l'expériences de plusieurs générations. Elles sont déterminées par les terres, le milieu, la région, la culture et la langue d'une communauté autochtone. Elles comprennent les connaissances provenant des générations passées, de même que les innovations et les nouvelles connaissances transmises aux générations futures.

Conservation numérique (ou archivage) : Gestion active au fil du temps d'un contenu numérique. Le processus inclut les activités suivantes : la sélection de contenus à préserver, la préparation et l'entretien de contenus dans un format ou dans un environnement propice à leur utilisation à long terme et la mise en place de stratégies pour assurer l'accessibilité des contenus à long terme.

Cycle de vie des données : Tous les stades d'existence de données à partir de la collecte jusqu'à la destruction. La perspective du cycle de vie permet la gestion active de données au fil du temps, pour en assurer ainsi la sécurité, l'accessibilité et l'utilité.

Dépersonnalisation (brouillage) : Le fait de modifier les données particulières liées à la personne afin de réduire le risque de divulgation de son identité. Cela peut

¹³ Réseau Portage (2020). *Boîte à outils pour les données sensibles destiné aux chercheurs - Glossaire terminologique sur l'utilisation des données sensibles à des fins de recherche*. Canadian Association of Research Libraries (CARL) / Association des bibliothèques de recherche du Canada (ABRC).

inclure le brouillage d'identificateurs directs (par exemple le nom, le numéro de téléphone, les coordonnées géographiques), la transformation (recodage, combinaison) ou la suppression d'identificateurs indirects qui pourraient être utilisés seuls ou en combinaison pour identifier une personne) par exemple, date d'anniversaire, coordonnées géographiques, dates d'événements clés).

Dépôt des données : Consignation de données dans un dépôt reconnu (institutionnel, national, code sources ouvert, dépôt par disciplines ou pluridisciplinaire ou autre) en vue de la conservation et possiblement de l'utilisation éventuelle par d'autres chercheurs ou chercheuses.

Domages : Conséquences négatives qui peuvent se traduire en effets indésirables sur les particuliers, les groupes ou les organismes. Les conséquences négatives peuvent être d'ordre social, comportemental, psychologique, économique, écologique ou légal. Elles peuvent porter atteinte à la vie privée, à la sécurité, à la réputation ou au statut d'une personne ou d'un organisme.

Données : Faits, mesures, enregistrements, archives ou observations sur le monde. Les données peuvent exister dans un format ou sur tout support. Elles peuvent prendre la forme d'écrits, de notes, de chiffres, de symboles, de textes, d'images, de films, de vidéos, d'enregistrements sonores, d'illustrations, d'esquisses, de dessins ou d'autres représentations graphiques, de reproductions, de manuels de procédures, de formulaires, de diagrammes, d'organigrammes de flux de travail, de descriptions d'équipement, de dossiers de données, d'algorithmes de traitement de données ou de registres statistiques.

Données anonymes : Données dépourvues d'identificateurs directs depuis la première collecte ; le risque d'identification à l'aide d'identificateurs indirects est faible et même très faibles. Sans évaluation en CÉR ; voir EPTC 2 (2022).

Données anonymisées (dépersonnalisées-brouillées) : Données dont les identificateurs directs ont été supprimés de manière irréversible ; aucun code n'est conservé qui pourrait permettre le recoupage futur avec des identificateurs directs ; le risque de réidentification de la personne à partir des identificateurs qui subsistent est faible et même très faible. Oblige l'évaluation en CÉR ; voir EPTC 2 (2022).

Données brutes : Données qui n'ont pas été interprétées en vue d'une utilisation pertinente. Les données brutes ont le potentiel de se transformer en « information », mais au préalable elles doivent être soumises à une extraction sélective et requièrent organisation, analyse et formatage avant d'être présentées. À moins d'être anonymes, les données brutes peuvent être considérées sensibles car elles ne sont pas dépersonnalisées.

Données comportant un niveau de risque élevé : Données qui nécessitent la mise en place de contrôles rigoureux contre la divulgation non autorisée, les pertes

ou les modifications de données susceptibles de porter atteinte tant aux chercheurs qu'aux participants de recherche, qui peuvent être des particuliers, des groupes ou des organismes. Les données qui comportent un niveau élevé de risque comprennent, mais non de façon limitative, des informations concernant la race ou l'origine ethnique ; les opinions politiques ; les croyances religieuses ou croyances de toute autre nature similaire ; l'affiliation syndicale ; la santé ou la condition physique ou mentale ; la vie sexuelle ; et l'infraction alléguée d'un délit par le participant.

Données comportant un niveau de risque faible : Données qui nécessitent la mise en place de contrôles contre les modifications de données non autorisées afin d'assurer l'intégrité des données plutôt que de prévenir les atteintes contre les chercheurs ou les participants de recherche. Les exemples comprennent, mais sans limitation, les données à accès libre composées de données entièrement dépersonnalisées ou anonymes, les formulaires de consentement en blanc, les fiches signalétiques et les données recueillies sur des sites Web destinés au public.

Données comportant un niveau de risque moyen : Données qui nécessitent la mise en place de contrôles rigoureux contre la divulgation non autorisée, les pertes ou les modifications de données ; dans la plupart des cas, ces données sont jugées confidentielles. La divulgation, la perte ou l'utilisation non autorisée de données confidentielles pourraient mettre en danger les participants. Des exemples de données confidentielles peuvent inclure les renseignements personnels identifiables (RPI), les renseignements personnels sur la santé (RPS) et les renseignements sur le crédit personnel (RPC).

Données confidentielles : Renseignements confiés à la personne, organisme ou personne morale responsable de maintenir le caractère privé de tels renseignements et de contrôler ou de restreindre l'accès à ceux-ci.

Données d'ordre administratif : Renseignements recueillis avant tout à des fins administratives et non à des fins de recherche. Sont compris dans cette catégorie les profils et les CV de chercheurs, la portée et l'impact de projets de recherche, les sources de financement, les citations et les résultats de recherche. Les renseignements de ce genre sont souvent recueillis par les services gouvernementaux et par d'autres organismes à des fins d'inscription, de transaction ou d'ouverture de dossiers liés à la prestation de services.

Données de recherche : Toute information recueillie, observée, générée ou créée soit en vue d'une recherche ou de la validation des résultats de recherche ; elles peuvent être répliquées ou réutilisées.

Données légalement accessibles : Données légalement accessibles au public, sous réserve de la nomination d'un gérant/dépositaire légalement désigné (voir gérant de données) qui assure la confidentialité et la protection des droits propriétaires des

données (par exemple, un coordonnateur d'accès à l'information ou consignataire des données du recensement canadien).

Données non identifiables : Données qui, dès la première collecte, ne peuvent pas être utilisées pour identifier un particulier, pour distinguer une personne par rapport à une autre ou pour retracer des informations personnelles identifiables.

Données ouvertes : Données disponibles en accès libre. Ce sont des données structurées qui sont accessibles, lisibles à la machine, utilisables, intelligibles et partageables gratuitement. Les données ouvertes sont gratuites et réutilisables. Elles se prêtent à la modification et à la distribution collective, sous réserve au maximum d'attribution-ShareAlike.

Données sensibles : Informations qui doivent être protégées contre l'accès non autorisé ou la divulgation. Elles peuvent inclure :

- Renseignements personnels
- Renseignements personnels sur la santé
- Dossiers scolaires
- Dossiers clients
- Informations financières
- Renseignements d'ordre criminel
- Renseignements géographiques
- Renseignements personnels conflictuels
- Renseignements jugés confidentiels ; données confiées à un tiers, à une organisation ou à une entité dans l'intention d'en préserver la confidentialité en interdisant ou en limitant les droits d'accès
- Renseignements protégés en vertu de toute politique interdisant l'accès non autorisé

Les données sensibles comprennent tout renseignement concernant une personne physique, une organisation ou une entité identifiée ou identifiable.

Entrepôt ou bibliothèque de données : Une localisation où les chercheurs peuvent consigner leurs données en vue de stockage et de gestion. Les entrepôts ou bibliothèques de données peuvent être sujets à des exigences particulières en matière de sujet, de domaine de recherche, de format et de réutilisation des données. Les documents consignés à l'entrepôt ou la bibliothèque de données font idéalement l'objet de curation, dont la responsabilité incombe au gérant des données qui doit assurer l'authenticité, le fait d'être facilement repérable et l'accessibilité à moyen terme.

EPTC 2 : L'Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains est une politique commune des trois organismes de recherche fédéraux (CRSH, CRSNG et IRSC).

Gérant de données : La personne responsable de la définition des données (c.-à-d. qui définit les traits particuliers d'éléments contenus dans la base de données) et de l'autorisation d'accès, surtout l'accès aux données ou la divulgation aux tierces personnes ; les gérants des données en collaboration avec les enquêteurs principaux fournissent du soutien pour :

- a) La collecte et l'intégration de données ou la réutilisation de données existantes ;
- b) Le contrôle de qualité des données ;
- c) La description du flux de travail / processus scientifique ;
- d) La fourniture de métadonnées conformes aux normes ; et
- e) La soumission et la production de données.

Après consultation et communication avec les enquêteurs principaux, les gérants de données sont responsables de :

- a) La préservation de données et de produits de données ; et
- b) La mise à disposition de modèles (par exemple, services Web, NetCDF, etc.) à des fins de découvert et d'intégration des données.

Gestion des données de recherche (GDR) : Processus dynamique impliquant la mise en œuvre de normes et de pratiques exemplaires au cours du cycle de recherche afin de maximiser l'efficacité et la réutilisabilité de données et de sous-produits connexes, y compris, mais non de façon limitative, les normes et les pratiques ayant trait à la gestion de données, la planification, les métadonnées, le stockage, l'émission de licences, l'éthique, la découverte, la conservation et la réutilisation.

Gestionnaire des données : Un informaticien ou un organisme spécialisé en informatique responsable de l'infrastructure informatique destinée à accueillir et à protéger des données conformément aux politiques et aux pratiques relatives à la gouvernance des données.

Logiciel de sondage en ligne : Logiciel utilisé par des chercheurs pour recueillir des données sur les répondants-participants à l'aide de questionnaires en ligne, dont les formulaires sont habituellement reliés à une base de données dans laquelle les réponses sont consignées et dont l'analyse est effectuée à l'aide des logiciels statistiques du produit. Il incombe tant aux chercheurs qu'aux participants de bien connaître les politiques en matière de confidentialité et de sécurité des données mises au point par les fournisseurs de ces logiciels.

Métadonnées : Signifient littéralement « données à propos de données » ; elles servent à définir ou à décrire les caractéristiques d'autres données. Le but étant de faciliter la compréhension des données et des processus ayant un lien avec les données.

Partage de données : Pratique qui consiste à rendre disponibles les données à des fins de découverte et de réutilisation. Pour en assurer l'accès, les données doivent être consignées dans un dépôt ou être publiées par tout autre moyen. Le partage peut faire l'objet de limitation ou autres conditions particulières, entre autres lorsque les données sont sensibles, sous réserve d'exigences ou lorsqu'elles sont protégées à titre de propriété exclusive.

Périphérique de stockage de données : Tout dispositifs ou support facilement transportable sur lequel les données peuvent être stockées. Cette définition n'est pas limitée aux périphériques conçus à cette fin comme les CD/ DVD, disques durs amovibles et clé USB, mais peut s'appliquer aux ordinateurs portables, tablettes électroniques, téléphones intelligents, PDA ou tout autre dispositif informatique. Les périphériques de stockage portables peuvent être connectés ou non connectés à Internet et les mesure de sécurité applicables seront variables selon le contexte.

Personne identifiable : Toute personne susceptible d'être identifiée directement ou indirectement, notamment par référence à un numéro d'identification ou par un ou plusieurs éléments qui sont spécifiquement liés à son identité physique, physiologique, mentale, économique, culturelle ou sociale. Même si on parle de « personnes » identifiables, les mêmes considérations sont applicables aux communautés, aux organismes et aux personnes morales.

Plan de gestion des données (PGD) : Énoncé formel décrivant comment les données de recherche seront gérées et documentées au cours d'un projet de recherche. Les éléments de base suivants sont normalement inclus dans le plan de gestion de données : les métadonnées. Les politiques régissant l'accès aux données, le partage, l'échange, la réutilisation et la répartition des données ; ainsi que les mesures visant le stockage, la conservation ou la destruction de données.

Pseudonymisation : Technique d'authentification ou utilisation d'un nom fictif (pseudonyme) pour désigner une personne, un groupe ou un lieu spécifique afin de supprimer tout lien ; le lien ne peut plus être établi en l'absence de renseignements supplémentaires. Dans le domaine de la recherche, la pseudonymisation est une sorte de dépersonnalisation pour protéger l'identité des participants et des organismes impliqués dans la recherche.

Publication des données : La divulgation des données de recherche, de métadonnées associées, de documentation d'appui et de code logiciel (dans les cas où les données brutes ont fait l'objet de traitement ou de manipulation) en vue d'une réutilisation ou d'une analyse, de telle manière qu'elles deviennent découvrables sur le Web et puissent être citées de manière unique et constante.

Renseignements disponibles au public : Tout matériel documentaire, enregistrement ou publication archivée existante qui peut comprendre ou non des renseignements identificatoires et qui

- a) N'a pas de restriction d'utilisation ou de distribution et ne comporte aucune attente raisonnable en matière de respect de la vie privée, particulièrement à l'égard de données de recherche avec des participants humains ; ou
- b) Qui peut être divulgué publiquement en vertu de mécanismes précis établis par règlement sous réserve de la nomination d'un gérant/ dépositaire désigné en conformité avec les lois sur l'accès à l'information et la protection de la vie privée, lequel doit assurer la confidentialité et la protection de droits propriétaires des données (par exemple, un coordonnateur d'accès à l'information et confidentialité ou consignataire des données du recensement canadien).

Renseignements identificatoires : Renseignements qui permettent d'identifier une personne, un organisme ou une personne morale ou qui risquent vraisemblablement de permettre de faire cette identification lorsque, en certaines circonstances ils sont utilisés seuls ou en combinaison avec d'autres renseignements. Ils peuvent être d'identification directe ou d'identification indirecte.

Renseignements personnels : Renseignements concernant une personne, y compris mais non de façon limitative :

- Nom, adresse ou numéro de téléphone,
- Race, nationalité ou origine ethnique, couleur, croyances religieuses ou politiques et affiliations à une association,
- Âge, genre, orientation sexuelle, état civil ou familial,
- Numéro d'identifiant, symbole ou autre signe attribué à une personne, symbole ou adresse protocole Internet (adresse IP), empreintes digitales, type sanguin ou traits héréditaires,
- Renseignements sur la condition de santé ou antécédents médicaux, y compris les conditions physique ou mentale,
- Renseignements sur l'éducation, les antécédents criminels, la condition financière ou statut d'emploi ou expérience professionnelle,
- Croyance, opinions, évaluations ou commentaires de la personne.

Il est à noter que l'évaluation concernant le risque d'identification des renseignements se fera dans le contexte d'un projet de recherche spécifique.

Renseignements personnels identifiables (RPI) : Semblables aux identificateurs directs, les RPI font référence à tout renseignement qui peut être utilisé pour identifier spécialement une personne, une organisation ou une entité (aux présentes la

« personne ») afin de contacter ou de retracer celle-ci, ou tout renseignement combiné avec d'autres sources de renseignement pour arriver au même objectif. Les RPI comprennent, mais non de façon limitative, le nom ou d'autres traits identificatoires de la personne comme la date d'anniversaire, l'adresse ou le géocodage. Les renseignements encodés à l'aide d'identificateurs personnels uniques peuvent être identificatoires si le détenteur des renseignements détient également la liste maîtresse ou la clé créant le lien entre les personnes et les identificateurs personnels uniques (IPU). Les renseignements peuvent également être identificatoires à ce niveau à cause de différents éléments d'identification connus à l'égard de cette personne. L'identité de la personne peut également être établie à partir de données agrégées, s'il n'y a qu'un nombre limité de personnes qui figurent dans cette catégorie. La capacité identificatoire est liée aux caractéristiques uniques des renseignements, à la quantité de renseignements détenus susceptibles d'être combinés ainsi qu'aux habiletés et technologies que le détenteur des renseignements pourrait déployer en vue de telles combinaisons.

Renseignements personnels sur la santé : Les renseignements identificatoires d'une personne de source orale ou de source écrite sont les suivants :

- a) Renseignements concernant la santé physique ou mentale d'une personne, y compris les renseignements au sujet de l'historique de santé de la famille,
- b) Renseignements concernant la prestation de soins de santé, incluant la personne qui en assure la prestation,
- c) Renseignements qui font partie d'un plan de service pour la personne au sens de La Loi sur les soins à domicile et les services communautaires (1994),
- d) Renseignements concernant les versements à la personne ou le droit de la personne aux soins de santé et à la prestation de soins de santé,
- e) Renseignements concernant le don par la personne de son corps ou d'une de ses substances corporelles ou tout renseignement provenant des résultats de tests ou d'examens effectués sur une partie du corps ou une substance corporelle de celui-ci,
- f) Le numéro d'assurance maladie de la personne ou,
- g) Les renseignements identifiant son décisionnaire remplaçant.

Il est à noter que l'évaluation concernant le risque d'identification des renseignements se fera dans le contexte d'un projet de recherche spécifique.

Renseignements primaires : Renseignements de première main recueillis par le chercheur (c.-à-d. directement des participants) concernant directement la question principale de la recherche.

Renseignements secondaires : Renseignements recueillis par une personne autre que le chercheur dans un but ne concernant pas directement la question principale de la recherche. Les renseignements secondaires sont des données préexistantes qui sont réutilisées dans un nouveau contexte qui est différent du contexte dans lequel les données ont été recueillies à l'origine.

Ressources destinées au public : Une ressource qui accepte les demandes anonymes d'accès à partir de toute adresse publique de protocole Internet, c'est-à-dire des ressources externes accessibles au public.

Risque : Éventualité de dommages ou d'atteintes qui peuvent être subis par des personnes, des communautés ou des organisations. Le risque est fonction de l'ampleur et de la gravité des dommages et de la probabilité de sa survenance chez les participants ou les tiers. En ce qui concerne le risque, il faut prendre en considération les dommages immédiats, les dommages différés et les dommages en aval.

Risques/dommages en aval : Conséquences négatives imprévues et inattendues au moment de la prise de décision, qui peuvent se traduire en effets indésirables sur les particuliers, les groupes ou les organismes. Au moment de la collecte de données sensibles, et en vue de leur conservation, entretien et réutilisation, les risques de dommages immédiats et en aval doivent être pris sérieusement en considération.

Sécurité des données : Moyens utilisés pour sauvegarder les données pour que le chercheur puisse y accéder de manière appropriée et selon ses besoins (disponibilité des données), de manière à ce qu'elles ne subissent aucune altération ou modification (intégrité des données), qu'elles demeurent confidentielles (confidentialité des données) et qu'elles soient soigneusement préservées et détruites (rétention/destruction).

Services infonuagiques : Une méthode de partage et d'enregistrement des données qui sont hébergées sur des serveurs à distance et accessibles par Internet. Les services infonuagiques sont hébergés, exploités et gérés par un fournisseur de services infonuagiques à partir d'un serveur d'archivage. Il existe des services infonuagiques publics et privés. L'utilisation de services infonuagiques comporte toujours un élément de risque, mais les risques associés aux serveurs publics ou privés sont d'un autre ordre. Les principales différences concernent la localisation, le contrôle du serveur ou des vulnérabilités potentielles.

- **Les services infonuagiques privés** assurent le stockage sur des serveurs internes à l'aide d'infrastructures locales ; aucun autre organisme n'a accès

aux services infonuagiques privés. La gestion et l'accès aux données sur des serveurs privés internes sont contrôlés par l'établissement, l'institution ou l'organisme responsable de l'infrastructure. Les données sont stockées sur l'intranet de l'institution et sont habituellement protégées par un pare-feu. La gestion, la conservation et la mise à jour de données relèvent de l'institution. Les services infonuagiques privés offrent souvent un niveau de sécurité plus élevé parce qu'il y a peu de mise en commun des ressources. Cependant, plusieurs établissements ne disposent pas de l'infrastructure et/ou du personnel pour héberger les services infonuagiques privés.

- **Les services infonuagiques publics** sont fournis par des entreprises qui offrent aux utilisateurs des services de stockage gratuits ou moyennant des frais sur des serveurs à distance gérés par le fournisseur. Le fournisseur est responsable de la gestion et de la conservation des données hébergées dans son centre de données. Si différents clients ont le droit d'utiliser les services infonuagiques publics, les données qui appartiennent aux clients et les applications que les clients font exécuter sur le nuage sont cachées aux autres utilisateurs du service infonuagique. À titre d'exemple de services infonuagiques publics, on peut nommer Google Drive, Drop Box, iCloud et OneDrive (personnel). Il convient de signaler aux établissements postsecondaires canadiens que les services infonuagiques publics sont offerts sur des serveurs qui échappent au contrôle de l'établissement. Les serveurs peuvent se trouver dans n'importe quel pays et, à ce titre, seront soumis aux lois du pays en question. Même si les services de nuage publics sont assortis de mesures de sécurité et de protection de la vie privée, ils demeurent vulnérables par l'étendue de leurs infrastructures et par la multitude de points d'accès à travers lesquels les utilisateurs non autorisés peuvent essayer de dérober des données. Dans certains contextes, les services infonuagiques privés sont moins vulnérables à de telles attaques.

Suppression : Le processus de destruction de données conservées sur des disques durs, sur des périphériques mobiles ou sur d'autres supports électroniques afin de les rendre illisibles, irrécupérables, inaccessibles ou inutilisables.

- Directeur des études
- Directrice des services financiers
- Directeur adjoint - Ressources informationnelles
- Responsable du service des communications, des affaires institutionnelles et de l'International
- Déploiement de la recherche

8. Bibliographie

- Alliance de recherche numérique du Canada à l'adresse électronique suivante : info@alliancecan.ca ou portage@carl-abrc.ca
- Association pour la recherche au collégial (ARC). (2018). *Consultation sur l'ébauche de la Politique des trois organismes sur la gestion des données de recherche : L'ARC mobilisée pour la gestion des données de la recherche collégiale.*
- Association pour la recherche au Collégial (ARC), <https://recherchecollegiale.ca/>
- Cégep de Lanaudière, *Stratégie de gestion des données de recherche.* [https://www.cegep-lanaudiere.qc.ca/sites/default/files/pages-regional/Recherche/strategie de gestion des donnees de recherche janvier 2023.pdf](https://www.cegep-lanaudiere.qc.ca/sites/default/files/pages-regional/Recherche/strategie%20de%20gestion%20des%20donnees%20de%20recherche%20janvier%202023.pdf)
- Cégep de Sherbrooke. (2023). *Stratégie institutionnelle de gestion des données de recherche.* [https://www.cegepsherbrooke.qc.ca/sites/default/files/strategie de gdr 10 janvier 2023.pdf](https://www.cegepsherbrooke.qc.ca/sites/default/files/strategie%20de%20gdr%2010%20janvier%202023.pdf)
- Cheung, M., Cooper, A., Dearborn, D., Hill, E., Johnson, E., Mitchell, M., & Thompson, K. (2022). Practices Before Policy: Research Data Management Behaviours in Canada. *Partnership: The Canadian Journal of Library and Information Practice and Research*, 17(1), 1–80. <https://doi.org/10.21083/partnership.v17i1.6779>
- Collège Laflèche, *Politique institutionnelle de la recherche.*
- Collège Laflèche, *Politique institutionnelle d'éthique de la recherche avec des êtres humains.*
- Collège Laflèche, *Politique institutionnelle sur la conduite responsable en recherche.*
- Collège Laflèche, *Politique institutionnelle sur les conflits d'intérêts en recherche.*
- CRSH, CRSNG et IRSC. (2022). *Politique des trois organismes sur la gestion des données de recherche.* <https://science.gc.ca/site/science/fr/financement-interorganismes-recherche/politiques-lignes-directrices/gestion-donnees-recherche/politique-trois-organismes-gestion-donnees-recherche>
- EPTC 2 (2022). *Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains est une politique commune des trois organismes de recherche fédéraux (CRSH, CRSNG et IRSC).*
- Réseau Portage (2020). *Partie 1 : Boîte à outils pour les données sensibles destiné aux chercheurs - Glossaire terminologique sur l'utilisation des données sensibles à des fins de recherche.* Canadian Association of Research Libraries (CARL) / Association des bibliothèques de recherche du Canada (ABRC).
- Réseau Portage (2020). *Partie 2 : Matrice de risque lié aux données de recherche avec des êtres humains.* Canadian Association of Research Libraries (CARL) / Association des bibliothèques de recherche du Canada (ABRC).
- Réseau Portage (2020). *Partie 3 : Langage en matière de gestion de données de recherche pour le consentement éclairé.* Canadian Association of Research Libraries (CARL) / Association des bibliothèques de recherche du Canada (ABRC).

- UNESCO, (2018). *Recommandation concernant la science et les chercheurs scientifiques*.
- Université Laval. (2022). *Stratégie institutionnelle pour la gestion des données de recherche*. <https://www.services-recherche.ulaval.ca/system/files/Documents/GDR/strategie-gestion-donnees-recherche.pdf>
- Université de Sherbrooke, (2022). *Stratégie institutionnelle en matière de gestion des données de recherche*. https://www.usherbrooke.ca/saric/fileadmin/sites/saric/documents/2-gestion/gestion_donnees_recherche/strategie-institutionnelle-gdr.pdf
- Université de Sherbrooke, (2022). *Politique sur la gestion des données de recherche*. <https://www.usherbrooke.ca/decouvrir/fileadmin/sites/decouvrir/documents/direction/politiques/2500-046.pdf>
- Université Saint-Anne. (2022). *Stratégie de gestion de données de recherche de l'Université Sainte-Anne*. <https://www.usaintanne.ca/actualites/publication-de-la-strategie-de-gestion-de-donnees-de-recherche-de-l-universite-sainte-anne>
- Université du Québec à Chicoutimi. (2019). *Stratégie institutionnelle de gestion de données de recherche*. https://docs.google.com/document/d/1cEZbKZ0uxZ8Q7SIvi5-5qmcnysKybur_2UUF9Supy4I/edit
- Université du Québec à Trois-Rivières. (2023). *Stratégie institutionnelle de gestion de données de recherche*. https://uqtr.libguides.com/ld.php?content_id=36686629 Au sujet des principes FAIR, l'UQTR référence l'URFIST Méditerranée. (2021). Les principes FAIR. <https://doi.org/10.13143/Z7S6-ED26>
- University of Virginia Library cite par Université Laval, (2022). *Stratégie institutionnelle pour la gestion des données de recherche*.
- Wilkinson, M. D., Dumontier, M., Aalbersberg, Lj. J., Appleton, G., Axton, M., Baak, A., ... Mons, B. (2016). The Fair Guiding Principles for Scientific data management and stewardship. *Scientific Data*, 3 160018. <https://www.nature.com/articles/sdata201618>