



DIRECTIVE D'UTILISATION DES RESSOURCES INFORMATIONNELLES

Adopté en septembre 2016
Révisé le 27 août 2024

Table des matières

Préambule	3
1 Définitions	3
2 Objectifs	4
3 Cadre légal et réglementaire	4
3.1 Cadre légal	4
3.2 Cadre administratif du Collège	5
4 Champ d'application	5
5 Utilisation des ressources informationnelles.....	5
5.1 Gestion des accès	5
5.1.1 Attribution des accès	6
5.1.2 Retrait ou suspension des accès	6
5.2 Messagerie électronique	7
6 Protection des ressources informationnelles	8
6.1 Par le Collège	8
6.2 Par l'utilisateur	9
6.3 Protection des documents	9
6.4 Renseignements personnels	10
6.5 Protection des équipements et des logiciels	10
7 Conditions complémentaires d'utilisation.....	10
7.1 Utilisation personnelle des ressources informationnelles	10
7.2 Utilisation interdite	10
8 Sanctions	11
9 Application de la directive	11
10 Entrée en vigueur.....	11

Préambule

La *Directive d'utilisation des ressources informationnelles* (ci-après la « **Directive** ») définit les responsabilités et les règles d'utilisation des ressources informationnelles, conformément à la *Politique de sécurité de l'information* et au *Cadre de gestion de la sécurité de l'information*.

Tout utilisateur est responsable de prendre connaissance de la présente Directive et de la mettre en application dans l'usage des ressources informationnelles mises à sa disposition par le Collège.

1 Définitions

Applications : Ensemble de programmes dont se servent les utilisateurs afin d'accomplir une tâche ou une activité.

Collège : Le terme Collège utilisé dans la présente directive s'applique aux activités se déroulant sur tous les campus ou à distance. Il signifie Collège de Maisonneuve.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

Document : Information fixée sur un support ; tout support d'information (papier, support magnétique, microforme, support optique numérique, etc.), y compris les données qu'il renferme, lisible par une personne ou par une machine.

Identifiant unique : Solution logicielle permettant aux utilisateurs d'un réseau d'accéder à l'ensemble des ressources autorisées sur la base d'une authentification multifacteurs. Les composantes de l'accès au réseau (code d'accès et mot de passe) sont confidentielles.

Infonuagique : Modèle informatique qui, par l'entremise de services distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, proposées sous forme de services évolutifs, adaptables et dynamiques.

Intégrité : Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

Plateforme infonuagique fournie par le Collège : Plateforme ayant été approuvée par le Collège pour le stockage d'information, qui est régie par un contrat avec le fournisseur de la plateforme, et qui est déployée et intégrée au sein de l'infrastructure des technologies de l'information du Collège.

Plateforme infonuagique publique : Plateforme infonuagique employée directement par l'utilisateur, qui n'est pas régie par le Collège et qui ne fait pas partie de son infrastructure des technologies de l'information. Les informations qui y sont enregistrées ne sont donc pas protégées par le Collège. Leur utilisation devrait être limitée à un usage personnel.

Réseau : Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations.

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.

Ressources informationnelles : Une ressource informationnelle est une ressource utilisée pour la réalisation d'activités d'enseignement, d'apprentissage, de recherche, de gestion et d'administration reliées à l'accomplissement de la mission du Collège, et des organismes dont il a la responsabilité. Les ressources informationnelles permettent la gestion, l'acquisition, le développement, l'entretien, l'exploitation, l'accès, l'utilisation, la protection, la conservation et la destruction des documents.

Sécurité informationnelle : Ensemble de mesures de sécurité physiques, logiques et administratives, et de mesures d'urgence mises en place dans une organisation, en vue d'assurer la protection de l'ensemble des ressources informationnelles. Plus particulièrement, la sécurité informationnelle assure l'intégrité, la confidentialité, l'authenticité, l'imputabilité et la fiabilité des documents et des systèmes.

Support de stockage : Support magnétique, optique ou électronique permettant de stocker des données de façon permanente.

Utilisateur : Tout membre du personnel du Collège de Maisonneuve (cadre, enseignant, professionnel, employé de soutien), tout étudiant, et toute personne physique ou morale qui agit comme sous-traitant, prestataire de service, contractant, collaborateur, partenaire ou autre pour le Collège, incluant les fournisseurs et les invités, autorisés à utiliser les ressources informationnelles.

2 Objectifs

La présente directive sur l'utilisation des ressources informationnelles vise à :

- Faire respecter les lois et les règlements en vigueur au Québec concernant les documents et les technologies de l'information.
- Assurer la sécurité informatique et la protection des ressources informationnelles du Collège.
- S'assurer que les renseignements personnels, les informations institutionnelles et la propriété intellectuelle du Collège soient protégés.
- Informer les utilisateurs de l'obligation de se servir des ressources informationnelles de manière responsable, empreinte de civilité et de respect.
- Régir les accès aux ressources informationnelles.

3 Cadre légal et réglementaire

3.1 Cadre légal

Le cadre légal de la présente directive est constitué, d'une part, par les lois canadiennes et québécoises en vigueur et, d'autre part, par les politiques et règlements propres au Collège.

- *Charte des droits et libertés de la personne, L.R.Q., c. C-12*
- *Code civil du Québec, L.Q. 1991, c-64*
- *Code criminel, L.R. 1985, ch. C-46*
- *Loi sur le droit d'auteur, L.R. 1985, ch. C-42*
- *Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1)*
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)*
- *Loi sur les archives (L.R.Q. c. A-21.1)*
- *Loi sur la gouvernance des ressources informationnelles des organismes publics et des entreprises du gouvernement*

3.2 Cadre administratif du Collège

- Le Projet éducatif
- Le Référentiel Être ensemble à Maisonneuve
- La Politique de gestion des ressources humaines
- La Politique sur la sécurité de l'information et le cadre de gestion de la sécurité de l'information
- La Politique sur la gestion documentaire
- La Politique relative à la protection des renseignements personnels
- La Politique de confidentialité lors de la collection de renseignements personnels par un moyen technologique
- Le Règlement sur les sanctions applicables en cas d'infractions à certaines conditions de vie au Collège
- La Directive de la gestion des identités et des accès (GIA)

4 Champ d'application

La présente directive s'applique à tous les utilisateurs des ressources informationnelles au Collège, c'est-à-dire tout membre du personnel du Collège de Maisonneuve, tout étudiant et toute personne physique ou morale, incluant les fournisseurs et les invités, autorisés à utiliser les ressources informationnelles.

5 Utilisation des ressources informationnelles

Les ressources informationnelles sont mises à la disposition des utilisateurs pour la réalisation d'activités d'enseignement, d'apprentissage, de recherche, de gestion et d'administration reliées à l'accomplissement de la mission du Collège, et des organismes dont il a la responsabilité.

5.1 Gestion des accès¹

¹ Pour plus d'informations, consultez la *Directive de gestion des identités et des accès*

5.1.1 Attribution des accès

La gestion des accès est encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de l'information soient strictement réservés aux personnes autorisées. Des mesures de sécurité sont prises par le Collège pour assurer la disponibilité, l'intégrité et la confidentialité de l'information.

L'accès au réseau se fait par le biais d'un identifiant unique attribué à l'utilisateur en fonction de son statut par la Direction des ressources informationnelles. Cet identifiant unique est assorti de permissions régissant les accès à des applications gérées par le Collège de Maisonneuve.

Le mot de passe doit être personnalisé selon les normes requises et conserve son caractère confidentiel. L'utilisateur ne doit, en aucun cas, communiquer, transmettre ou dévoiler son identifiant à un autre utilisateur ou à un tiers.

L'accès à certaines applications requiert des identifiants uniques spécifiques. L'utilisateur sera informé des modalités lorsque les accès seront autorisés.

Seules les personnes ayant obtenu du Collège un identifiant sont autorisées à utiliser les ressources informationnelles auxquelles cet identifiant donne accès. Pour le personnel, la demande d'attribution des accès doit être approuvée par le supérieur immédiat.

5.1.2 Retrait ou suspension des accès

Les accès octroyés à un utilisateur peuvent en tout temps être résiliés sans préavis si celui-ci contrevient au cadre légal et réglementaire en vigueur ou s'il y a menace pour la sécurité du Collège ou d'un tiers.

Pour les employés :

Lorsqu'un employé quitte définitivement le Collège, ses accès sont désactivés à la fin de la dernière journée de travail. Tous les documents enregistrés sur des répertoires personnels (ex. : OneDrive) ainsi que sa messagerie électronique seront supprimés, et ce, sans aucun droit de recours de sa part.

Lorsqu'un employé est absent pour une invalidité d'un mois ou plus, tous ses accès, y compris à la messagerie, seront suspendus jusqu'à son retour.

Lorsqu'un employé s'absente pour un départ non définitif (congé parental, congé sans salaire, congé différé par exemple) ou s'il est suspendu, les accès de l'employé seront suspendus à la fin de sa dernière journée de travail et resteront inaccessibles jusqu'à son retour, y compris l'accès à la messagerie.

Lorsqu'un employé accède à un nouveau poste (changement de poste), l'ensemble de ses accès seront révoqués et de nouveaux accès lui seront octroyés selon ses nouvelles fonctions à la demande de son supérieur immédiat.

Pour les étudiants :

L'étudiant inscrit au Collège possède un identifiant unique.

Lorsqu'il n'est plus inscrit depuis deux sessions consécutives au Collège, son identifiant est détruit. S'il se réinscrit, un nouvel identifiant lui est alloué.

Lorsque l'étudiant est diplômé, ses accès sont révoqués et l'identifiant est détruit.

5.2 Messagerie électronique

L'utilisateur qui obtient une adresse de courrier électronique du Collège doit utiliser l'application de messagerie électronique gérée par le Collège.

Seule l'adresse courriel du Collège de l'utilisateur sera utilisée pour les communications organisationnelles

L'utilisateur fait usage de mesures de protection et de sécurité adéquates lors de la transmission de documents, de renseignements personnels ou confidentiels, ainsi que d'informations à caractère stratégique pour le Collège.

Le téléchargement d'information à partir d'Internet ou l'ouverture de pièces jointes dans les courriers électroniques doivent être faits avec soin afin d'éviter l'exécution de code malveillant.

Les communications doivent, en tout temps, être respectueuses avec tous les interlocuteurs. Les propos injurieux, diffamatoires, haineux ou pouvant constituer une forme de menace, de harcèlement, de dénigrement ou de discrimination sont interdits.

Dans toute communication, l'utilisateur s'identifie avec sa signature et en aucun cas il ne doit tenter d'usurper l'identité d'un autre utilisateur ou celle d'un tiers. Il est interdit d'utiliser un moyen détourné pour transmettre un courriel de façon anonyme ou au nom d'une autre personne.

Si un employé est absent pour une courte ou longue période, le responsable hiérarchique peut solliciter l'accès à sa boîte de messagerie, sous réserve de l'approbation de la direction du service des ressources humaines.

5.3 Appareils mobiles

5.3.1 Cellulaire²

Le besoin d'utiliser un appareil mobile (cellulaire) comme outil de travail doit être préalablement déterminé par le supérieur immédiat et validé par le directeur du service selon les besoins du poste.

Le cellulaire sera remplacé au rythme du plan de remplacement prévu (généralement aux 3 ans) et selon les disponibilités budgétaires.

L'employé devra respecter les limites d'utilisation des forfaits négociés par le Collège ou son mandataire. Dans le cas où la limite est dépassée, avec les justificatifs et l'approbation du supérieur immédiat, le

² Pour plus d'informations, consultez le cadre de gestion des cellulaires

Collège prendra en charge les frais encourus. Sans justification et approbation du supérieur immédiat, le Collège émettra une facture d'utilisation à l'employé.

Dans le cas où une utilisation de l'appareil est faite à l'extérieur du réseau du fournisseur de services prévu au forfait, des frais d'itinérance seront facturés. Ces frais ne sont pas inclus dans le forfait proposé par le Collège.

Les données personnelles conservées sur l'appareil mobile sont de la responsabilité de l'utilisateur. En aucun cas, le Collège ne peut être tenu responsable de la perte, du vol ou de la mauvaise utilisation de ces données. Il est de la responsabilité de l'utilisateur de prendre les précautions nécessaires comme faire des copies de sauvegarde.

5.3.2 Ordinateur portable

L'utilisation d'un ordinateur portable est justifiée pour les personnes qui sont en télétravail ou se déplacent régulièrement, après validation par la direction du service.

L'enseignant au régulier ou CFC (charge formation continue) ayant une tâche équivalente ou supérieure à 60% annuellement peut faire la demande d'un portable.

L'acquisition et le remplacement des ordinateurs portables seront faits annuellement lors de la planification du MAOB et selon les disponibilités budgétaires.

6 Protection des ressources informationnelles³

6.1 Par le Collège

Le Collège met en place des procédures et assure la protection des ressources informationnelles. La Direction des ressources informationnelles protège les systèmes d'information jugés comme étant essentiels à la bonne marche des activités du Collège contre les menaces qui peuvent survenir et qui ont le potentiel d'affecter la confidentialité, l'intégrité, la disponibilité, l'usage prévu et la valeur de ces systèmes.

L'approche utilisée tient compte des changements qui peuvent être soudains afin de soutenir la prestation continue des services. La protection contre les menaces informatiques et technologiques nécessite la mise en place de mesures spécifiques pour protéger le réseau du Collège. Ceci exige que la Direction des ressources informationnelles procède à des contrôles sécuritaires permettant d'effectuer une surveillance en continu afin d'identifier et d'analyser les menaces, ainsi qu'établir des mécanismes efficaces pour réduire et contrer ces menaces.

³ Pour plus d'informations, consultez la Politique de sécurité de l'information

Les responsabilités des intervenants en matière de sécurité de l'information sont définies dans le cadre de gestion de la sécurité de l'information.

Lorsqu'un utilisateur se voit attribuer des ressources informationnelles (équipements informatiques, cellulaires, etc.), celles-ci demeurent la propriété du Collège. Les autorisations et la gestion de ces ressources se font dans les mêmes conditions que la gestion des accès.

6.2 Par l'utilisateur

L'utilisateur se comporte de manière prudente et responsable dans l'utilisation des ressources informationnelles mises à sa disposition.

L'utilisateur :

- Respecte et applique les mécanismes de sécurité des fichiers, des banques de données ou d'information, des ordinateurs, des systèmes ou des réseaux et ne tente pas de les violer ou de les rendre vulnérables;
- Respecte les consignes de restriction d'accès et ne peut introduire ni faciliter l'accès à des personnes non autorisées dans les locaux ayant un accès restreint.
- Respecte les consignes d'utilisation des équipements, des logiciels et des licences;
- Respecte la réglementation des réseaux externes et de l'intégrité des systèmes auxquelles il accède par l'utilisation des équipements informatiques du Collège;
- Gère ses mots de passe et ses codes d'accès de façon confidentielle.

Tout utilisateur est tenu de rapporter promptement les incidents de sécurité et le non-respect de la présente directive par un autre utilisateur aux responsables identifiés.

L'utilisateur qui fait usage de ressources informationnelles personnelles, comme un ordinateur portable ou un téléphone cellulaire, est responsable de les utiliser de façon responsable et sécuritaire lorsqu'il accède aux ressources informationnelles du Collège. Il doit s'assurer de sauvegarder les documents relatifs à ses activités au Collège sur les supports de stockage du Collège.

6.3 Protection des documents

Le Collège assure l'archivage centralisé des documents des utilisateurs sur les supports de stockage du Collège.

L'utilisateur est responsable des documents dont il fait usage. Il s'assure que tous les messages et documents numériques créés ou reçus par courrier électronique, qui ont trait à ses activités au Collège, sont sauvegardés conformément à la *Politique sur la gestion documentaire*.

Les documents enregistrés sur un poste multiutilisateur ont une durée éphémère et seront supprimés périodiquement.

L'utilisateur qui conserve des documents personnels sur un poste de travail qui lui a été attribué réalise lui-même les copies de sauvegarde. Il ne peut invoquer la responsabilité du Collège pour la perte ou la destruction de documents qui ne seraient pas sur les supports de stockage du Collège.

6.4 Renseignements personnels

L'information contenue dans les ressources informationnelles est confidentielle lorsqu'elle a un caractère de renseignement personnel ou d'un renseignement que le Collège protège en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) ou d'un renseignement relatif à la vie privée de la personne au sens du *Code civil du Québec* (L.Q. 1991, c-64).

L'utilisateur a la responsabilité de protéger les renseignements personnels qu'il détient contre la perte ou le vol, et contre l'accès, la divulgation, la copie, l'utilisation ou la modification non autorisés par la loi ou contraires à sa Politique relative à la protection des renseignements personnels. L'utilisateur faisant usage d'un poste multiutilisateur, y compris dans les laboratoires informatiques ou les ordinateurs portables empruntés à la bibliothèque, s'assure de ne pas y laisser de documents contenant des renseignements personnels.

6.5 Protection des équipements et des logiciels

Aucune altération ou modification aux ressources informationnelles n'est permise.

Il est interdit de déplacer les ordinateurs ou les périphériques sans l'autorisation de la Direction des ressources informationnelles.

L'utilisateur qui s'est vu attribuer un privilège d'administrateur des éléments logiciels sur son poste de travail utilise ce privilège de manière responsable. Il fait en sorte que les ajouts et les modifications qu'il effectue à son poste de travail n'altèrent pas les fonctionnalités de celui-ci. En cas d'incident, la responsabilité de la Direction des ressources informationnelles est de remettre le poste fonctionnel en rétablissant la configuration d'origine du poste.

7 Conditions complémentaires d'utilisation

7.1 Utilisation personnelle des ressources informationnelles

Il est permis aux utilisateurs d'utiliser les ressources informationnelles du Collège à des fins personnelles, dans la mesure où cet usage ne nuit pas aux exigences de travail ou d'études, ne requiert pas l'utilisation de ressources humaines et matérielles supplémentaires, et ne déroge en aucune façon à la présente directive ou à toute autre loi.

Le collège se garde le droit d'accéder à ses équipements en cas de besoin.

7.2 Utilisation interdite

Toute utilisation des ressources informationnelles du Collège à des fins illégales ou de quelque manière incompatible avec la mission éducative du Collège, est strictement interdite.

Toute utilisation commerciale, à des fins autres que la mission du Collège, est interdite.

Il est interdit d'accéder aux systèmes du Collège et de les utiliser en tentant de masquer son identité. En tout temps, la Direction des ressources informationnelles doit être en mesure d'identifier l'auteur d'une transmission circulant sur son réseau.

La liste des comportements répréhensibles est incluse dans le *Règlement sur les sanctions applicables en cas d'infractions à certaines conditions de vie au Collège*, à l'annexe A : Liste de comportement répréhensible.

8 Sanctions

Tout manquement à la présente directive peut entraîner l'application de sanctions selon la nature des gestes faits. Ces sanctions seront imposées conformément aux conventions collectives ou à la *Politique de gestion du personnel-cadre*, si le contrevenant est un employé du Collège, et conformément au *Cadre de référence relatif aux conditions de vie au Collège*, si le contrevenant est un étudiant, un invité ou un fournisseur.

Des plaintes ou des recours appropriés ainsi que des réclamations en dommages pourront être portés devant la justice contre toute personne tenue responsable de gestes relevant d'une utilisation malveillante et illégale des ressources informationnelles du Collège ou en contravention à la *Charte des droits et libertés de la personne*.

9 Application de la directive

La présente directive est placée sous la responsabilité de la Direction des ressources informationnelles.

La Direction des communications et du développement institutionnel est chargée de la diffusion auprès de tous les utilisateurs. L'autorité administrative de chaque unité est responsable de la sensibilisation des utilisateurs dans leur usage des ressources informationnelles.

La mise en œuvre et le respect de la présente Directive incombent à chaque utilisateur.

10 Entrée en vigueur

La directive entre en vigueur dès son adoption par le comité de direction.