CÉGEP Heritage COLLEGE

23

CÉGEP HERITAGE COLLEGE
POLITIQUE N° 23

SUR LES
RÉSEAUX NUMÉRIQUES

EN VIGUEUR : **Le 28 septembre 1999**

RÉVISÉE : **Le 19 juin 2024**
Le 17 septembre 2025

ADMINISTRATION : **Directeur du Service des technologies de l'information**

POLITIQUE N^{O} 23 DU CÉGEP HERITAGE COLLEGE SUR LES RÉSEAUX NUMÉRIQUES

Préambule[1,2]

Le Cégep Heritage College (nommé ci-après le « Cégep ») offre à ses personnes étudiantes et à son personnel l'accès à ses réseaux numériques, qui constituent une ressource essentielle. Ces réseaux sont conçus pour soutenir la réalisation de la mission et des objectifs éducatifs du Cégep. Ils favorisent une communication innovante et un partage responsable de l'information au sein de la communauté collégiale, améliorent l'éducation publique et encouragent les valeurs du développement durable. En tant qu'élément central de l'infrastructure numérique de l'établissement, Internet relie le Cégep à un écosystème mondial de connaissances. Ce réseau facilite la recherche, la sensibilisation du grand public et l'engagement citoyen, et renforce la visibilité ainsi que la réputation du Cégep.

Conscient que l'utilisation des réseaux numériques comporte à la fois des possibilités et des risques, le Cégep adopte une approche de gouvernance fondée sur la responsabilisation, la transparence et l'innovation éthique. La présente Politique s'aligne sur les cadres juridiques, réglementaires et politiques suivants :

- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises publiques (RLRQ, c. G-1.03)*,
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1)* (la « *Loi 25* »), et
- La *Loi sur les archives (RLRQ, c. A-21.1)*.

En intégrant ces obligations dans son cadre de gouvernance numérique, le Cégep veille à ce que ses réseaux et ses systèmes intégrant l'intelligence artificielle soient utilisés de manière à protéger les droits individuels, à maintenir l'intégrité institutionnelle, à promouvoir la transparence et la confiance, et à respecter toutes les normes juridiques et éthiques applicables. La présente Politique favorise un environnement numérique responsable qui contribue à la réalisation des objectifs éducatifs et opérationnels du Cégep.

ARTICLE 1
Objectif

La présente Politique vise à définir des attentes claires en matière d'utilisation acceptable des réseaux numériques du Cégep. Elle décrit les activités autorisées et précise les comportements interdits afin d'éviter toute utilisation abusive susceptible de mettre en péril les activités du Cégep ou d'entraîner des responsabilités juridiques.

ARTICLE 2
Dispositions générales

Les réseaux numériques du Cégep sont accessibles aux personnes étudiantes, au personnel et aux autres personnes autorisées pour des activités directement liées aux fonctions académiques et administratives. L'utilisation personnelle est autorisée, pourvu qu'elle ait lieu pendant le temps libre, qu'elle n'occasionne pas de coûts supplémentaires et qu'elle ne comporte pas de gain financier. Toutes les activités du réseau doivent être conformes à la présente Politique et tout manquement fera l'objet de mesures appropriées, dans les meilleurs délais et en toute équité.

ARTICLE 3
Champs d'application

La présente Politique s'applique à tous les membres de la communauté du Cégep qui ont accès aux ressources du réseau numérique, y compris le personnel, les personnes étudiantes, les visiteurs et les personnes qui entretiennent une relation de travail ou de service avec le Cégep. Son application couvre l'accès aux systèmes et services qui exploitent ou interagissent avec l'intelligence artificielle (IA), tels que les outils de prise de décision automatisés, les modèles d'apprentissage automatique, les plateformes d'IA générative et les systèmes académiques ou administratifs basés sur l'IA.

[1] Dans le présent document, la forme masculine sera réputée comprendre tous les genres sans aucune discrimination dans le seul but d'alléger le texte. Le singulier comprend le pluriel et le pluriel le singulier.

[2] Consulter le « Glossaire » afin de trouver les explications des termes fréquemment utilisés.

La présente Politique s'étend également aux situations d'accès à distance, y compris le télétravail et d'autres activités hors campus, où les ressources numériques du Cégep ou les services recourant à l'IA sont utilisés. Toute personne qui utilise les réseaux numériques est tenue d'interagir avec ces technologies conformément aux valeurs institutionnelles, à la législation applicable et aux normes d'utilisation responsable définies par la présente Politique et les lignes directrices provinciales pertinentes.

ARTICLE 4
Utilisations autorisées et interdites des réseaux numériques

4.1 Utilisations autorisées

La présente section définit les activités autorisées sur les réseaux numériques du Cégep, dans le but de soutenir les objectifs opérationnels et pédagogiques de l'établissement. Tous les membres de la communauté du Cégep sont tenus d'utiliser les ressources numériques de manière responsable et éthique, dans le respect des politiques institutionnelles et des normes légales applicables. Les activités suivantes illustrent les usages autorisés, sous réserve du respect des lignes directrices énoncées :

4.1.1 Activité professionnelle et scolaire

- **Fonctions professionnelles et académiques :** L'utilisation des ressources numériques pour s'acquitter des responsabilités professionnelles, académiques ou de recherche qui lui sont confiées, conformément aux objectifs stratégiques du Cégep.
- **Collaboration et communication :** Le partage d'informations avec des collègues, des personnes étudiantes, des partenaires publics, et des contacts professionnels, à condition que ces échanges ne compromettent pas la confidentialité, la vie privée ou la sécurité institutionnelle.
- **Développement professionnel :** L'accès à des activités de formation approuvées, telles que des cours en ligne ou des webinaires, favorisant le développement des compétences liées à son rôle.

4.1.2 Utilisation responsable des ressources

- **Logiciels et outils approuvés :** L'acquisition ou utilisation de logiciels, de plateformes infonuagiques ou d'applications sous licence ou approuvés par l'établissement qui contribuent à l'enseignement, l'apprentissage ou l'efficacité opérationnelle.
- **Utilisation personnelle raisonnable :** L'utilisation personnelle limitée des ressources numériques pendant le temps libre est autorisée à condition qu'elle ne nuise pas au travail, ne mobilise pas de ressources de façon excessive et ne contrevienne pas aux politiques du Cégep.

4.2 Activités interdites

Toute utilisation des réseaux numériques du Cégep qui compromet la cybersécurité, enfreint les lois applicables ou contrevient aux politiques du Cégep est interdite. La participation à l'une des activités interdites énumérées ci-dessous peut entraîner des mesures disciplinaires pouvant aller jusqu'à la résiliation de l'accès, le renvoi du Cégep, des poursuites judiciaires et des accusations criminelles, le cas échéant. Les activités interdites comprennent, sans s'y limiter :

4.2.1 Sécurité et confidentialité

- **Transmission non sécurisée :** La transmission des renseignements personnels à caractère confidentiel, y compris les renseignements personnels, sur des réseaux non sécurisés est strictement interdite, sauf s'ils sont chiffrés conformément aux normes de sécurité du Cégep. Les réseaux non sécurisés désignent les réseaux externes au Cégep. Lorsque des utilisateurs accèdent aux ressources du Cégep ou transmettent des données sensibles depuis l'extérieur des locaux, ces personnes sont tenues d'utiliser le réseau privé virtuel (RPV) approuvé par le Cégep afin de garantir la sécurité des communications.

- **Accès non autorisé :** La tentative d'accéder, d'utiliser ou de partager des données, des systèmes ou des comptes sans autorisation expresse.
- **Violation de la sécurité :** La tentative de contourner, de désactiver ou de compromettre les contrôles de sécurité tels que les pares-feux, la détection des intrusions ou le chiffrement.

4.2.2 Intégrité du réseau et son utilisation

- **Abus de ressources :** Les activités qui perturbent ou dégradent les performances du réseau, telles que les envois massifs de courriels, le minage infonuagique non autorisé, ou la diffusion en continu excessive.
- **Logiciels non autorisés :** L'installation, le téléchargement, ou l'utilisation de logiciels, d'applications ou de périphériques non approuvés susceptibles de compromettre l'intégrité du système.
- **Distribution de logiciels malveillants :** Le téléchargement, l'hébergement, ou la propagation de virus, rançongiciels, logiciels espions ou autres logiciels malveillants.

4.2.3 Contenu et normes

- **Contenu illégal ou inapproprié :** Créer, accéder, stocker, ou distribuer du contenu obscène, pornographique, abusif, ou violent.
- **Communication abusive ou discriminatoire :** Il est interdit d'envoyer des messages ou des contenus abusifs, sexistes, racistes, menaçants, à caractère harcelant, diffamatoires ou autrement discriminatoires ou offensants, à l'égard d'une personne ou un groupe.

4.2.4 Représentation et expression

- **Assertions inexactes :** Faire passer des points de vue personnels comme s'il s'agissait de propos approuvés ou tenus par le Cégep, sans l'autorisation explicite du Directeur général, porte atteinte à l'intégrité du Cégep et est interdit.
- **Activité politique et critique publique :** Il est interdit d'utiliser les ressources du Cégep pour participer à des activités politiques ou pour critiquer publiquement les politiques ou les actions du gouvernement de façon à laisser entendre que le Cégep y souscrit, à moins que ces activités ne soient directement liées aux responsabilités pédagogiques ou professionnelles de la personne concernée et qu'elles soient approuvées par le Directeur général.

4.2.5 Activités illégales

- **Cybercriminalité :** Se livrer à des activités de piratage, d'accès non autorisé, de destruction ou de modification de données, de diffusion de logiciels malveillants, ou à toute autre activité visant à compromettre la sécurité des systèmes et réseaux informatiques.
- **Violations de la propriété intellectuelle :** Enfreindre les droits d'auteur, les marques commerciales ou les brevets d'autrui sans autorisation**.**
- **Fraude et activités illégales :** Utiliser le réseau pour commettre des actes de fraude, d'extorsion, de corruption, de jeux d'argent illégaux, ou d'autres actes criminels.

ARTICLE 5
Surveillance

5.1 Objectif de la surveillance

Le Cégep est chargé de veiller au respect de la présente Politique ainsi que des autres politiques institutionnelles et exigences légales. En raison de cette obligation, il est essentiel de reconnaître que la surveillance des activités du réseau numérique est une composante nécessaire de ses stratégies de gouvernance et de sécurité.

5.2 Qu'est-ce qui est surveillé?

- **Trafic sur le réseau et flux de données :** Il s'agit notamment de surveiller le volume de données transmises, la durée des sessions et les types de protocoles utilisés. Elle permet de gérer la bande passante du réseau et de détecter des anomalies susceptibles d'indiquer des menaces pour la sécurité ou des usages abusifs.
- **Journaux d'accès :** Le Cégep tient des journaux détaillés des accès au système et au réseau, comprenant les identifiants des utilisateurs, les horodatages, les périphériques utilisés et la nature des données consultées. Ces informations sont essentielles à des fins d'audit et peuvent servir à enquêter sur des violations de la présente Politique ou des infractions.
- **Systèmes de courrier électronique et de communication :** Toutes les communications entrantes et sortantes font l'objet d'un contrôle de conformité aux normes juridiques et aux politiques institutionnelles, notamment en ce qui concerne les contenus malveillants, le pourriel et le partage d'informations non autorisé.
- **Accès aux fichiers et aux ressources :** La surveillance des accès aux ressources est essentielle pour s'assurer que les informations sensibles ou confidentielles ne sont pas consultées ou partagées de manière inappropriée. Elle comprend l'analyse en temps réel des comportements d'accès et la vérification des droits d'accès.
- **Activités et comportement des utilisateurs** : La surveillance en temps réel des actions sur le réseau, soit les téléchargements, l'accès à des sites Web et l'utilisation de logiciels, vise à garantir le respect des politiques d'utilisation acceptable et à prévenir la diffusion de contenus interdits.
- **Systèmes et contrôles de sécurité :** Des vérifications régulières de l'efficacité des mesures de cybersécurité, notamment les pares-feux, les systèmes de détection d'intrusion et les outils de lutte contre les logiciels malveillants, sont effectuées afin de s'assurer qu'ils fonctionnent conformément aux attentes.

5.3 Considérations relatives à la protection de la vie privée

Bien que la surveillance soit essentielle à des fins opérationnelles et de sécurité, le Cégep s'engage à respecter la vie privée de tous les utilisateurs du réseau. Les activités de surveillance sont conformes aux lois et règlements applicables en matière de protection des renseignements personnels, notamment la *Charte des droits et libertés de la personne* et la *Loi 25*. Les informations obtenues dans le cadre de la surveillance du réseau sont utilisées strictement à des fins de conformité, de sécurité et d'efficacité opérationnelle, et sont traitées de manière confidentielle.

5.4 Signalement et intervention en cas d'incident

Les constats issus des activités de surveillance qui révèlent des violations de la présente Politique ou des incidents de sécurité sont documentés et traités conformément aux procédures d'intervention en cas d'incident. Cette procédure prévoit notamment la notification immédiate des autorités compétentes au sein du Cégep et, s'il y a lieu, des autorités policières ou judiciaires compétentes.

ARTICLE 6
Accès à l'information

Le Cégep veille à ce que tous les journaux d'activité du réseau soient conservés dans le strict respect des protocoles de confidentialité et de sécurité. Ces journaux détaillent les sites Web visités, les destinataires des courriels et l'identité des appareils du service ou du département à l'origine de ces contacts. L'accès à ces journaux et à l'information y afférente est accordé dans des conditions spécifiques afin de maintenir l'intégrité et la sécurité des réseaux numériques du Cégep et de se conformer aux exigences légales et réglementaires.

6.1 Maintenance et sécurité des journaux d'activité du réseau

Le Cégep s'engage à maintenir rigoureusement les journaux d'activité du réseau, dans le respect des normes les plus strictes en matière de confidentialité et de protocoles de sécurité. Ces journaux enregistrent

systématiquement les sites Web visités, les destinataires des courriels et l'identification des appareils à l'origine de ces contacts au sein de l'infrastructure du réseau du Cégep. La gestion de ces journaux est essentielle pour maintenir l'intégrité et la sécurité de ses réseaux numériques et pour garantir le respect des cadres juridiques et réglementaires en vigueur.

6.2 Conditions d'accès à l'information

L'accès à ces journaux détaillés et aux données associées est strictement contrôlé et autorisé dans les conditions spécifiques suivantes afin de préserver l'intégrité du réseau et de se conformer aux obligations légales :

6.2.1 Constats lors de la surveillance courante

Lors de la surveillance courante du réseau, si des anomalies ou des activités suspectes sont détectées et indiquent des menaces potentielles pour la sécurité ou des violations de la présente Politique, le personnel désigné du STI est autorisé à accéder aux journaux et aux données pertinents. Cet accès est uniquement destiné à mener des enquêtes et à mettre en œuvre des mesures correctives pour remédier à ces problèmes.

6.2.2 Demandes d'enquête interne

Le Cégep peut, dans des circonstances nécessitant des enquêtes internes liées au respect des politiques d'emploi ou à la suite d'allégations d'inconduite professionnelle, demander l'accès à des journaux de réseau et à des communications en particulier. L'accès dans ces conditions sera régi par les principes de nécessité et de proportionnalité, en veillant à ce qu'il soit limité à l'information pertinente pour l'enquête en cours.

6.2.3 Demandes licites des autorités

L'accès aux journaux de réseau peut également être accordé en réponse à des demandes licites émanant des autorités policières, judiciaires ou gouvernementales compétentes. Dans ces cas, le Cégep s'engage à respecter pleinement les lois, en veillant à ce que toute communication d'information soit effectuée dans le strict respect des normes juridiques et des exigences réglementaires établies.

6.3 Obligations en matière de conformité et de protection de la vie privée

Le Cégep reconnaît ses obligations légales et éthiques de fournir un accès aux documents du réseau dans les cas déterminés par la présente Politique. Toutes les procédures relatives à l'accès à l'information du réseau sont rigoureusement encadrées afin de concilier le besoin de sécurité et l'impératif de protection de la vie privée et des renseignements sensibles. Ces procédures font partie intégrante de l'engagement du Cégep à respecter les normes juridiques et les responsabilités institutionnelles dans la gestion de ses ressources d'information numérique.

ARTICLE 7
Formation obligatoire en cybersécurité

7.1 Exigences en matière de formation

Le Cégep impose une formation complète en cybersécurité à l'ensemble de son personnel afin de renforcer le niveau de sécurité de l'organisation contre les cybermenaces. Cette formation vise à doter le personnel et les personnes étudiants des connaissances et des compétences actualisées nécessaires à la protection des ressources numériques personnelles et institutionnelles.

7.1.1 Cours de mise à jour annuelle

L'ensemble du personnel et des personnes étudiants en informatique est tenu de participer à des formations annuelles de mise à niveau portant sur les dernières pratiques en matière de cybersécurité, la sensibilisation aux menaces et les mesures préventives.

7.1.2 Simulations trimestrielles d'hameçonnage

Afin de renforcer la sensibilisation à l'hameçonnage et les capacités d'intervention, le Cégep organisera des simulations trimestrielles pour l'ensemble du personnel. Ces simulations sont essentielles pour évaluer l'état de préparation et offrir une formation immédiate aux personnes qui donnent suite par inadvertance à des tentatives d'hameçonnage.

7.2 Conformité et voies de remédiation

Le non-respect des exigences en matière de formation à la cybersécurité peut compromettre la position du Cégep en matière de sécurité. Des voies de remédiation particulières sont établies pour ce qui suit :

7.2.1 Remédiation en cas d'inachèvement de la formation

Le personnel et les personnes étudiantes qui n'ont pas suivi les séances de formation obligatoires dans le délai imparti feront l'objet des mesures suivantes :

- **Premier palier du recours hiérarchique :** Les cas de non-conformité sont d'abord portés à la connaissance du superviseur immédiat de la personne concernée.
- **Deuxième palier du recours hiérarchique :** Si la non-conformité continue, le directeur du service concerné est saisi.
- **Mesure finale :** En cas de non-conformité persistante, la situation est portée à l'attention du Directeur général pour la prise les mesures qui s'imposent.

7.2.2 Mesures correctives en cas d'échec aux simulations d'hameçonnage

Pour les personnes qui sont victimes de simulations d'hameçonnage :

- **Formation immédiate :** Une formation corrective immédiate est dispensée pour remédier aux vulnérabilités ciblées.
- **Simulation de suivi :** Une simulation subséquente est réalisée pour s'assurer de la bonne compréhension et de l'application de la formation. D'autres échecs peuvent donner lieu à des séances de formation supplémentaires.

7.3 Évaluation et mise à jour des formations

L'efficacité du programme de formation en cybersécurité est régulièrement évaluée. La rétroaction des participants est essentielle pour mettre à jour et perfectionner les modules de formation afin de répondre à l'évolution des défis en matière de cybersécurité.

7.4 Obligations juridiques et éthiques

Le Cégep reconnaît ses responsabilités juridiques et éthiques en ce qui concerne l'imposition d'une formation rigoureuse à la cybersécurité. Le respect de ces exigences de formation est essentiel pour maintenir l'intégrité des données personnelles et institutionnelles et pour se conformer aux normes juridiques applicables.

ARTICLE 8
Utilisation acceptable de l'intelligence artificielle (IA)

L'utilisation d'outils et de plateformes d'IA sur les réseaux et appareils numériques du Cégep n'est autorisée que lorsqu'elle respecte les principes de transparence, de responsabilisation, d'équité, de confidentialité et de respect des droits individuels. L'utilisation de l'IA doit servir la mission et les valeurs du Cégep, se conformer à toutes les lois et politiques applicables, et être menée de manière à protéger les renseignements personnels, l'intégrité intellectuelle et la réputation de l'établissement.

8.1 Finalité et alignement

L'IA peut être utilisée pour faire progresser la mission du Cégep en matière d'éducation, de recherche, d'administration et d'innovation. Son utilisation doit favoriser l'apprentissage et la réussite étudiante,

renforcer les normes les plus élevées en matière d'intégrité intellectuelle et refléter l'éthique, l'équité et l'inclusion institutionnelles. Toutes les activités liées à l'IA doivent être conformes à la législation québécoise, y compris la Loi 25 sur la protection des renseignements personnels.

8.2 Utilisations interdites

Les utilisations suivantes de l'IA sont strictement interdites :

- **Fraude académique :** Utiliser l'IA pour tricher, plagier, induire en erreur ou nuire de toute autre manière à l'intégrité académique, conformément à la Politique n° 5 sur l'Évaluation de la réussite étudiante.
- **Tromperie et désinformation :** Générer ou diffuser des contenus faux, trompeurs ou préjudiciables susceptibles de nuire à la confiance du grand public, à la réputation du Cégep ou à l'intégrité de l'enseignement et de la recherche.
- **Violations de la propriété intellectuelle :** L'utilisation de l'IA d'une manière qui enfreint les droits d'auteur, les marques de commerce ou d'autres droits de propriété intellectuelle.
- **Surveillance ou profilage non autorisés :** La surveillance, le profilage ou analyse de personnes sans leur consentement ou une autorisation légale.
- **Violations de la sécurité :** L'utilisation de l'IA pour compromettre la sécurité du réseau, obtenir un accès non autorisé à des informations ou perturber les activités du Cégep.
- **Harcèlement ou discrimination :** La génération ou l'amplification de contenus harcelants, discriminatoires ou incompatibles avec les valeurs de diversité, d'équité et d'inclusion du Cégep. Est également visée la création ou la diffusion d'hypertrucage, d'usurpations d'identité ou d'autres formes de médias synthétiques susceptibles d'induire en erreur, de diffamer ou de nuire aux membres de la communauté du Cégep ou au grand public.

8.3 Transparence et divulgation

Lorsque l'utilisation de l'IA est autorisée dans un cours pour aider à la création d'un travail académique ou créatif, cette utilisation doit être clairement divulguée. Les personnes étudiantes et le personnel doivent respecter les exigences de déclaration énoncées dans la Politique N° 5 sur l'Évaluation de la réussite étudiante, y compris l'attribution et la reconnaissance appropriées des contributions de l'IA. Le personnel enseignant et l'administration sont chargés d'établir des lignes directrices disciplinaires concernant l'utilisation acceptable de l'IA dans des contextes académiques ou opérationnels. Le fait de ne pas déclarer l'utilisation de l'IA lorsque cela est requis constitue un manquement à la responsabilité académique ou professionnelle.

8.4 Confidentialité et protection des données

Les utilisateurs ne doivent pas saisir des renseignements personnels, confidentiels ou sensibles du Cégep dans des outils d'IA publics ou tiers, y compris les dialogueurs d'IA générative. Sont notamment visés les données relatives aux personnes étudiantes, au personnel, aux dossiers scolaires, aux opérations internes ou toute autre information protégée par la législation sur la protection des renseignements personnels ou les politiques du Cégep.

Aux fins de la présente Politique, et conformément à la *Loi 25*, on entend par « renseignements personnels » toute information qui se rapporte à une personne physique et qui permet de l'identifier, directement ou indirectement. Il peut s'agir de noms, de numéros d'identification, de coordonnées, de données biométriques ou de renseignements sur la santé, ou de toute combinaison d'éléments de données permettant d'identifier raisonnablement une personne.

8.5 Imputabilité

Les utilisateurs sont entièrement responsables des conséquences de leur utilisation de l'IA, y compris de l'exactitude, de la fiabilité et des implications éthiques des résultats. Une utilisation négligente ou inappropriée de l'IA peut entraîner des mesures disciplinaires en vertu des politiques du Cégep, y compris

des sanctions académiques pour les personnes étudiantes et des mesures administratives ou disciplinaires liées à l'emploi pour le personnel.

8.6 Utilisation institutionnelle et approbation des outils

L'achat, le déploiement ou l'intégration d'outils d'IA dans les systèmes, services ou opérations du Cégep nécessite une évaluation et une approbation préalables par le STI. Le STI évalue la sécurité, la conformité, la confidentialité, l'accessibilité et les risques éthiques avant d'autoriser l'utilisation institutionnelle de l'IA. L'intégration non autorisée de l'IA dans les systèmes du Cégep est interdite.

ARTICLE 9
Demandes d'information sur la politique

Toute demande concernant la mise en œuvre, l'interprétation ou l'application de la présente Politique doit être adressée au Directeur du STI. Ce dernier est désigné comme point de contact principal pour répondre aux questions et aux précisions souhaitées par les utilisateurs des réseaux numériques du Cégep. Ce protocole garantit l'uniformité des communications et le respect des dispositions de la présente Politique.

ARTICLE 10
Mesures disciplinaires

10.1 Signalement et traitement des incidents

10.1.1 Signalement d'incident

Tout service ou département identifiant des activités soupçonnées d'être illégales ou interdites dans le cadre du réseau numérique doit en informer sans délai le Directeur du STI. Ce dernier est tenu d'évaluer et de documenter le signalement, puis d'acheminer le dossier au service compétent pour qu'il en assure le suivi.

10.1.2 Escalade et participation des autorités

Dès réception d'un signalement, le Directeur général évalue la nécessité de prendre d'autres mesures, y compris le renvoi de l'affaire aux autorités policières ou judiciaires compétentes aux fins d'enquête et de poursuites éventuelles. Cette escalade est entreprise lorsqu'elle est jugée nécessaire, en fonction de la gravité et de la nature de l'infraction.

10.1.3 Mesures correctives

Que l'affaire soit ou non portée devant les autorités compétentes, le Cégep se réserve le droit d'imposer des mesures internes pouvant donner lieu à des sanctions disciplinaires. Ces mesures peuvent être engagées indépendamment du statut ou de l'issue de toute procédure criminelle ou de tout litige civil pouvant découler des activités signalées.

10.2 Conséquences d'une violation de la Politique

Le non-respect de la présente Politique fait l'objet de mesures disciplinaires strictes, qui reflètent la gravité de l'infraction et ses répercussions sur les activités et la réputation du Cégep. Les mesures disciplinaires peuvent notamment comprendre ce qui suit :

- **Refus temporaire ou permanent d'accès au réseau :** Les utilisateurs peuvent se voir refuser l'accès aux réseaux numériques du Cégep de manière temporaire ou permanente, en fonction de la gravité de l'infraction.
- **Congédiement ou de résiliation de l'inscription :** Dans les cas les plus graves, les violations de la présente Politique peuvent entraîner le congédiement ou la résiliation de l'inscription de la personne concernée. Cette mesure est envisagée lorsque la violation entraîne des répercussions sur la situation juridique du Cégep, sur sa position en matière de cybersécurité ou sur la confiance à un point tel que la poursuite de l'emploi ou de la relation scolaire ne peut être maintenue.

Le Cégep s'engage à maintenir un environnement numérique sécurisé et conforme à la loi. Tous les membres de la communauté du Cégep sont tenus d'observer pleinement la présente Politique et les procédures établies pour signaler et traiter les infractions.

ARTICLE 11
Rôles et responsabilités

11.1 Conseil d'administration

Le Conseil d'administration est chargé d'approuver la présente Politique et ses révisions ultérieures.

11.2 Directeur générale

Le Directeur général est chargé de l'application de la présente Politique et des mesures disciplinaires liées aux signalements d'activités inacceptables ou illégales, le cas échéant.

11.3 Directeur du Service des technologies de l'information (STI)

Le Directeur du STI est chargé de la mise en œuvre et de l'application de la présente Politique au Cégep. Cette responsabilité comprend ce qui suit :

- **Application de la politique :** Établir et maintenir des pratiques solides au sein du Cégep afin de garantir le respect permanent de la présente Politique.
- **Enquêtes :** Superviser les enquêtes relatives à tout signalement d'activités inacceptables ou illégales menées par des utilisatrices ou des utilisateurs des réseaux numériques du Cégep, en coordination avec d'autres services, départements ou organismes externes, si nécessaire, afin de traiter et de résoudre efficacement ces situations.
- **Principes et objectifs :** Définir les principes et les objectifs généraux de la présente Politique, en veillant à ce qu'elle soutienne les objectifs stratégiques du Cégep en veillant à ce qu'elle soutienne les objectifs stratégiques du Cégep et soit conforme à toutes les lois et à tous les règlements applicables.

Le Directeur du STI est chargé de l'examen et de la révision continus de la présente Politique afin d'en garantir la pertinence et l'efficacité. Le processus de révision a lieu en fonction de l'évolution des considérations juridiques, techniques et opérationnelles ou, au minimum, tous les trois ans à compter de la date de son adoption. Des révisions seront entreprises pour tenir compte des évolutions technologiques, des modifications des exigences légales ou d'améliorations procédurales.

11.4 Haute direction

La haute direction du Cégep est chargée de responsabilités particulières en ce qui concerne le respect de l'intégrité de la présente Politique :

- **Sensibilisation et éducation :** Veiller à ce que tous les utilisateurs au sein de leurs services ou départements respectifs soient pleinement informés de la présente Politique, en comprennent les implications et soient conscients des conséquences de son non-respect.
- **Filtrage de sécurité :** Superviser les processus de vérification afin de s'assurer que tous les utilisateurs disposent des autorisations nécessaires avant d'accéder aux systèmes, réseaux ou applications sensibles.
- **Résiliation de l'accès :** Faciliter la suppression rapide de l'accès au réseau pour les personnes qui ne sont plus employées ou affiliées au Cégep, protégeant ainsi l'information et les ressources sensibles contre toute utilisation ou tout accès non autorisé.

11.5 Évaluation de la conformité et de l'efficacité

La haute direction doit évaluer le respect de la présente Politique et son efficacité dans le cadre du processus de planification annuelle du Cégep. Cette évaluation est essentielle pour cerner les axes d'amélioration et garantir que la présente Politique reste efficace dans la gestion des risques associés à l'utilisation des réseaux numériques.

11.6 Responsabilités de l'utilisateur

11.6.1 Obligation de se conformer

Le respect de la présente Politique est obligatoire pour toutes les personnes étudiantes, le personnel, et les visiteurs et les personnes qui entretiennent une relation de travail ou de service avec le Cégep autorisée à utiliser le réseau numérique du Cégep. Cette exigence s'applique à toute personne qui utilise les réseaux numériques dans le cadre de ses activités au Cégep.

11.6.2 Connaissance et reconnaissance

Chaque utilisateur doit prendre connaissance des dispositions de la présente Politique avant d'avoir accès aux réseaux numériques du Cégep. À cette fin, chacun doit :

- **Prise de connaissance de la Politique :** S'engager à comprendre la portée, les dispositions et les implications de la présente Politique dans le cadre de son rôle et de ses responsabilités au sein du Cégep.
- **Engagement formel** : Remplir et signer le « Formulaire de contrat d'utilisation » (Document de référence N^{o} P23.1), qui peut être obtenu auprès du STI du Cégep. Ce formulaire constitue une reconnaissance formelle de la compréhension et de l'acceptation de la présente Politique par l'utilisateur, et affirme son engagement à en respecter les dispositions et les restrictions à chaque accès au réseau.

ARTICLE 12
Révisions

La présente Politique sera révisée tous les cinq (5) ans ou lorsque cela sera jugé nécessaire.

GLOSSAIRE

Activité acceptable : Ceci implique l'utilisation par les personnes étudiantes, le personnel, chaque service, chaque département, et autres personnes autorisées pour exercer des activités au nom du Cégep (voir l'article 4.1).

Activité illégale : Comprend les infractions criminelles, les contraventions aux lois fédérales et provinciales de nature réglementaire non criminelle, et les actions qui rendent une personne étudiante, un membre du personnel, un représentant autorisé, ou les services et départements responsables d'une poursuite civile ou de procédures criminelles (voir les articles 4.2 et 4.3).

Communauté du Cégep : Le terme comprend le personnel, les personnes étudiantes, les parents/tuteurs, le Conseil d'administration, et les visiteurs et les personnes qui entretiennent une relation de travail ou de service avec le Cégep.

Hypertrucage : Ce terme désigne tout contenu visuel, audio ou vidéo produit ou altéré artificiellement à l'aide de l'intelligence artificielle ou de techniques d'apprentissage automatique, afin de faire croire à tort qu'une personne dit ou fait quelque chose qu'elle n'a en réalité ni dit ni fait.

Intelligence artificielle : Ce terme désigne les systèmes, les logiciels ou les technologies capables d'effectuer des tâches qui requièrent généralement l'intelligence humaine. Ces tâches peuvent inclure l'apprentissage, le raisonnement, la résolution de problèmes, la prise de décision, la compréhension du langage ou la génération de contenu.

Piratage : Il s'agit de la pratique consistant à exploiter les faiblesses d'un système informatique, d'un réseau, d'une application ou d'un dispositif numérique afin d'obtenir un accès non autorisé, de mener des activités malveillantes ou de manipuler le comportement du système.

Renseignements personnels identifiables : Ce terme désigne toute information permettant d'identifier directement ou indirectement une personne. Cela inclut à la fois les identifiants directs (par exemple, le nom au complet, le numéro d'assurance sociale, le numéro d'étudiant, le numéro de permis de conduire, l'adresse courriel, le numéro de téléphone) et les identifiants indirects qui, combinés, pourraient révéler l'identité d'une personne (par exemple, la date de naissance, le code postal, le sexe ou d'autres données démographiques).

Réseaux numériques : Groupes d'ordinateurs et de systèmes informatiques qui peuvent communiquer entre eux. Sans restreindre la portée générale de ce qui précède, ces réseaux comprennent Internet, les réseaux internes à l'établissement et les réseaux publics et privés externes à l'établissement.

Surveillance : La consignation et l'analyse des transactions d'information et de contrôle qui ont lieu sur les réseaux numériques..

Utilisateur : Toute personne ou entité qui interagit avec un système informatique, une application logicielle, un réseau, ou un service numérique.

Documents connexes

Le présent document doit être utilisé conjointement avec les documents suivants :

- La *Charte québécoise des droits et libertés de la personne (RLRQ, c C-12)*[3]
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c G-1.03)*[4]
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c A-2.1)*[5]
- Le Code de conduite éthique du Cégep Heritage College[6]
- La Politique N^{o} 48 sur les Renseignements personnels et la confidentialité du Cégep Heritage College[7]
- La Politique N° 6 sur un Environnement respectueux, exempt de discrimination et de harcèlement du Cégep Heritage College [8]
- La Politique N^{o} 22 sur la Gestion des documents et des archives du Cégep Heritage College [9]
- La Politique N° 24 sur les Normes de conduite étudiante du Cégep Heritage College [10]
- La Procédure N^{o} 40 relative à la Divulgation d'actes répréhensibles du Cégep Heritage College[11]

[3] Des copies de ce document sont disponibles auprès de la Direction générale.
[4] Ibid.
[5] Ibid.
[6] Des copies de ce document sont disponibles auprès de la Direction générale et sur le site Web du Cégep.
[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] Ibid.
[11] Ibid.

Documents de référence

- Document de référence N^{o} P23.1 - Formulaire de contrat d'utilisation pour les personnes étudiantes
- Document de référence N^{o} P23.2 - Formulaire de contrat d'utilisation pour le personnel
- Document de référence N^{o} P23.3 - Formulaire d'autorisation de dérogation (le personnel)