



FÉLIX-LECLERC | GABRIELLE-ROY | LOUIS-REBOUL

Gatineau, Qc

RÈGLEMENT RELATIF À L'UTILISATION DU PARC INFORMATIQUE ET MULTIMÉDIA PAR LE PERSONNEL

DU CÉGEP DE L'OUTAOUAIS

Campus Gabrielle-Roy

333, boul. de la Cité-des-Jeunes
Gatineau, QC J8Y 6M4

Campus Félix-Leclerc

820, boul. de la Gappe
Gatineau, QC J8T 7T7

Campus Louis-Reboul

125, boul. Sacré-Coeur
Gatineau, QC J8X 1C5



**RÈGLEMENT RELATIF À L'UTILISATION DU PARC INFORMATIQUE ET MULTIMÉDIA
PAR LE PERSONNEL DU CÉGEP DE L'OUTAOUAIS**

Notes chronologiques :	Règlement adopté en vertu de :
Adopté le 28 novembre 2011 au conseil d'administration (CA-468.14). Abrogé le 9 juin 2026 au conseil d'administration (CA-601.19).	La Charte des droits et libertés de la personne (L.R.Q., c. C-12) Le Code civil du Québec (L.Q. 1991, c. C-64) La Loi sur le droit d'auteur (L.R.C. (1985), ch. C-42) Le Code criminel (L.R.C. (1985), ch. C-46) La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., C.A-2.1)

Table des matières

RÈGLEMENT RELATIF À L'UTILISATION DU PARC INFORMATIQUE ET MULTIMÉDIA PAR LE PERSONNEL DU CÉGEP DE L'OUTAOUAIS

PRÉAMBULE	4
ARTICLE 1 FINALITÉ.....	4
ARTICLE 2 DÉFINITIONS	4
ARTICLE 3 CADRE JURIDIQUE	5
ARTICLE 4 RESPONSABILITÉS DE L'UTILISATRICE OU DE L'UTILISATEUR	6
4.1 Utilisation de l'ensemble du parc informatique.....	6
4.2 Accès au réseau du Cégep et à son contenu.....	7
4.3 Informations des personnes utilisatrices.....	8
4.4 Modification des équipements informatiques	9
4.5 Messagerie électronique	10
ARTICLE 5 RESPONSABILITÉS DU CÉGEP	11
5.1 Confidentialité des informations	11
5.2 Sécurité des données sur le réseau	11
5.3 Protection des systèmes informatiques	11
5.4 Renseignements protégés	11
5.5 Protection contre les logiciels malveillants	12
5.6 Vérification.....	12
5.7 Droit d'auteur.....	12
ARTICLE 6 SANCTIONS.....	12
6.1 Restrictions d'utilisation.....	12
6.2 Sanctions disciplinaires	12
ARTICLE 7 CYBERSÉCURITÉ ET PROTECTION DES DONNÉES	12
7.1 Formation et sensibilisation	12
7.2 Sécurité d'accès et authentification à facteurs multiples.....	12
7.3 Mise à jour et gestion des vulnérabilités.....	12
7.4 Chiffrement et protection des échanges	13
7.5 Surveillance et détection des incidents.....	13
ARTICLE 8 APPLICATION DU RÈGLEMENT	13
ARTICLE 9 PARTAGE DES RESPONSABILITÉS	13
ARTICLE 10 ENTRÉE EN VIGUEUR.....	13
ARTICLE 11 RÉVISION DU RÈGLEMENT	13

PRÉAMBULE

Le présent Règlement définit les règles relatives à l'utilisation de l'ensemble du parc informatique et multimédia mis à la disposition des usagers par le Cégep de l'Outaouais. Il vise à garantir la qualité, la sécurité et la pérennité des ressources numériques, tout en protégeant les investissements de l'établissement et en assurant le respect des obligations légales et réglementaires de celui-ci. Dans un contexte de menaces numériques croissantes et d'exigences accrues en matière de protection des données, ce document intègre désormais des dispositions relatives à la cybersécurité, à la sécurisation des échanges et à la gestion des incidents. Il intègre également une disposition habilitante permettant d'encadrer par voie de directives l'utilisation des outils d'intelligence artificielle, dont l'évolution rapide requiert une agilité réglementaire particulière.

ARTICLE 1 FINALITÉ

Le présent règlement a pour objet d'établir le cadre d'utilisation des équipements informatiques et multimédias, de prévenir les usages abusifs ou illicites et de définir les comportements attendus en vue de préserver l'intégrité, la confidentialité et la disponibilité des ressources technologiques du Cégep.

ARTICLE 2 DÉFINITIONS

Dans le présent *Règlement*, on entend par :

Bande passante (débit binaire) : Nombre maximal d'éléments binaires transmis par seconde sur une voie de transmission. Dans le cas spécifique d'Internet, le Cégep de l'Outaouais achète, chaque année, un débit binaire selon l'évaluation de ses besoins annuels.

Espace réseau du Cégep : Sa fonction principale est de stocker, d'organiser et de rendre accessibles des fichiers et des données aux utilisateurs ou aux appareils-clients connectés à un réseau. Deux types de stockage réseau sont utilisés au Cégep : le stockage sur serveur local et le stockage infonuagique (Microsoft OneDrive et SharePoint). Le contenu entreposé sur l'espace réseau et sur l'espace OneDrive et SharePoint appartenant aux membres du personnel est sauvegardé pour une période de 1 an, tandis que le contenu appartenant aux comptes étudiants est disponible pendant 30 jours après son effacement. Le plan de sauvegarde pour les données des utilisateurs peut être appelé à changer afin de suivre les meilleures pratiques de l'industrie.

Identifiant réseau : Un identifiant réseau est la combinaison de son code d'accès individuel alloué par le Cégep et d'un mot de passe confidentiel.

Liste de distribution : Liste d'adresses de courrier électronique de personnes utilisatrices créée pour des fins spécifiques, propres à la poursuite de la mission du Cégep. De telles listes peuvent, par exemple, être créées par programme, par service, etc.

Contenu protégé obtenu illégalement : Tout matériel distribué de façon commerciale, notamment les logiciels, progiciels, didacticiels, médias numériques de nature textuelle, sonore ou visuelle, ou toute banque de données et d'informations, installé ou utilisé sur les équipements informatiques et dont le Cégep ne possède pas les droits ou les licences d'utilisation et de diffusion.

Données sensibles : Informations personnelles, confidentielles ou stratégiques nécessitant une protection particulière.

Authentification à facteurs multiples (AFM) : Processus d'identification d'une personne requérant plusieurs éléments de vérification pour renforcer la sécurité d'accès à nos systèmes.

Incident de cybersécurité : Tout événement susceptible de compromettre l'intégrité, la confidentialité ou la disponibilité des systèmes informatiques.

Membre du personnel technique à la Direction en charge des ressources informationnelles ou un délégué : Personne désignée qui, dans le cadre de ses fonctions dans un service ou un département du Cégep, exerce le contrôle ou la gestion, ou effectue les opérations sur la partie du parc informatique sous sa responsabilité.

Outil d'intelligence artificielle (IA) : Tout système logiciel utilisant des techniques d'apprentissage automatique ou de traitement du langage naturel pour générer, analyser ou transformer du contenu, accessible via une plateforme SaaS ou intégré à un logiciel institutionnel (ex. : assistants de rédaction, générateurs d'images, outils de synthèse).

Parc informatique ou équipement informatique : Comprend notamment, mais non sans s'y limiter :

- tout équipement informatique ou relatif au système informatique, comprenant tout poste de travail informatisé, ordinateur (peu importe son format et la présence de capacité réseau ou non), imprimante, moniteur, projecteur, téléviseur, câble, clavier, station d'accueil, ainsi que tout accessoire ou unité informatique, dont ceux servant à la réception, au traitement, à la conservation, à la reproduction et à la transmission d'informations et de données;
- tout équipement qui permet l'accès au réseau Internet/Intranet ou qui est relatif au système d'accès au réseau Internet/Intranet, en branchement filaire ou sans fil;
- tout équipement qui permet l'accès au courrier électronique ou relatif au système de courrier électronique;
- tout logiciel, progiciel, didacticiel, document ou les bases des données et d'informations (textuelles, sonores ou visuelles) placé dans un équipement ou sur un média informatique connecté à l'équipement;
- le nom de domaine cegepoutaouais.qc.ca, ses sous-domaines lui appartenant et leur contenu.

Personne administratrice du parc informatique : Personne désignée qui, dans le cadre de ses fonctions à la Direction des ressources informationnelles du Cégep, exerce le contrôle ou la gestion du parc informatique et multimédia.

Utilisatrice ou utilisateur : Toute personne employée par l'établissement, les membres du conseil d'administration, toute la communauté étudiante, ainsi que toute personne physique ou morale autorisée à utiliser les équipements informatiques.

Signature modèle du Cégep : Fichier texte de quelques lignes inséré à la fin d'un message électronique et permettant d'identifier le Cégep d'une manière cohérente à son image corporative.

Système d'exploitation : Logiciel permettant la gestion des différents éléments matériels de l'ordinateur et l'utilisation des logiciels.

Logiciel en tant que service – SaaS: C'est un modèle de distribution de logiciels où l'application n'est pas installée sur l'ordinateur de l'utilisateur, mais hébergée sur des serveurs distants et accessible via Internet, généralement au moyen d'un navigateur web.

ARTICLE 3 CADRE JURIDIQUE

L'utilisation des technologies de l'information doit se faire en conformité avec la législation en vigueur, notamment en vertu des lois suivantes :

- la Charte des droits et libertés de la personne (L.R.Q., c. C-12);
- le Code civil du Québec (RLRQ c CCQ-1991);
- la Loi sur le droit d'auteur (L.R.C. (1985), ch. C-42);
- le Code criminel (L.R.C. (1985), ch. C-46);
- la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., C.A-2.1);
- la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.Q., chapitre G-1.03)
- la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (LQ 2021, c. 25 ou la « Loi 25 »)

- la Loi canadienne anti-pourriel (Loi C-28)
- les licences, ententes de groupe signées par le Cégep;

tous les règlements, politiques et directives en vigueur au Cégep.

ARTICLE 4 RESPONSABILITÉS DE L'UTILISATRICE OU DE L'UTILISATEUR

4.1 Utilisation de l'ensemble du parc informatique

4.1.1 Conditions générales d'utilisation

La vocation première du parc informatique doit être d'appuyer la poursuite de la mission pédagogique et administrative du Cégep en tant qu'établissement d'enseignement. Le Cégep en autorise l'usage responsable à des fins privées, à condition que cet usage soit occasionnel, qu'il se déroule à l'extérieur des heures de prestation de travail ou de services, qu'il n'affecte pas la productivité, n'entraîne pas de coûts supplémentaires pour le Cégep et qu'il demeure en tout temps conforme aux dispositions du présent *Règlement*. Aucun soutien ne sera donné pour les logiciels (portables ou infonuagiques), les sites internet et le matériel informatique (ordinateur ou téléphone intelligent) qui est utilisé à des fins privées (personnelles) ou pour du matériel qui n'appartient pas au Cégep.

4.1.2 Utilisation d'Internet

Le Cégep fournit aux personnes utilisatrices l'accès à Internet. Lorsqu'elles utilisent l'Internet, celles-ci doivent respecter les règles suivantes :

- l'utilisation d'Internet est, en principe, limitée à des fins professionnelles. Le Cégep en autorise l'usage exceptionnel à des fins privées, à condition que cet usage soit occasionnel, se déroule à l'extérieur des heures de prestation de travail ou de services, n'affecte pas la productivité, n'entraîne pas de coûts supplémentaires pour le Cégep, et qu'il demeure, en tout temps, conforme aux dispositions du présent *Règlement*;
- il est strictement interdit de diffuser ou télécharger des données protégées par tout droit de propriété intellectuelle, en violation des lois applicables. Aucune personne utilisatrice ne peut se servir des outils d'accès à Internet pour télécharger ou distribuer tout matériel contenu protégé obtenu illégalement;
- sauf dans le cadre d'activités pédagogiques reconnues, il est strictement interdit de consulter des sites Internet dont le contenu est susceptible de porter atteinte à la dignité d'autrui, de consulter des sites à caractère érotique ou pornographique, prônant la discrimination sur la base du sexe, de l'orientation sexuelle, du handicap, de la religion, de la race ou de l'origine nationale ou ethnique. Le Cégep se réserve également le droit de bloquer, à tout moment et sans avertissement préalable, l'accès aux sites Internet dont il juge que le contenu est non conforme aux dispositions de ce *Règlement*.

Les flux de données entrants et sortants de l'Internet et l'Intranet sont surveillés, vérifiés, stockés et analysés par nos systèmes de surveillance réseau, notre service de surveillance active SOC et d'autres partenaires comme le RISQ, CIRA et le ministère de la Cybersécurité et du Numérique du Québec.

4.1.3 Utilisation à des fins commerciales

Toute utilisation du parc informatique et multimédia à des fins commerciales autres que celles reliées aux activités institutionnelles ou parascolaires reconnues du Cégep est interdite sans l'autorisation de la Direction générale.

4.1.4 Utilisation des jeux électroniques et vidéo

Sauf dans le cadre d'activités pédagogiques ou parascolaires reconnues, il est interdit d'installer ou d'utiliser, sur les équipements informatiques, tout jeu électronique ou vidéo, incluant ceux disponibles par les fureteurs Web, sans autorisation préalable d'un administrateur du parc informatique.

4.1.5 Utilisation des réseaux sociaux

L'utilisation responsable du clavardage en ligne (*chat*), forums de discussion et réseaux sociaux est permise, à condition que cet usage se fasse dans le cadre d'activités pédagogiques reconnues, ou soit

occasionnel, qu'il se déroule à l'extérieur des heures de prestation de travail ou de services, qu'il n'affecte pas la productivité, n'entraîne pas de coût supplémentaire pour le Cégep et qu'il demeure en tout temps conforme aux dispositions du présent *Règlement*.

L'utilisation des réseaux sociaux est soumise aux mêmes principes guidant l'utilisation de la messagerie électronique : l'utilisateur doit s'y identifier en tant qu'elle-même et ne pas tenter d'usurper l'identité d'une autre personne. Elle doit y utiliser un langage courtois et de qualité supérieure.

Il est en outre interdit de recourir à un vocabulaire injurieux, malveillant, haineux ou discriminatoire, ou se livrer à toute forme de harcèlement, de menace, d'intimidation ou de diffamation. De même, en vertu du principe de loyauté envers l'employeur, il est interdit pour toute personne salariée de tenir des propos jugés inappropriés envers son employeur.¹

4.1.6 Utilisation de la bande passante

Par souci d'équité, l'utilisation de la bande passante doit se faire avec discernement. L'utilisation des services de diffusion vidéo en continu (*streaming*), contenu télévisuel et vidéoconférence, est exclusivement réservée aux activités pédagogiques, administratives et parascolaires reconnues.

Sauf dans le cadre d'activités pédagogiques ou administratives reconnues, la présence sur le réseau informatique du Cégep de serveurs de partage de données non autorisés tels que les logiciels utilisant des protocoles pair-à-pair (*peer-to-peer*), des serveurs de partage de fichiers (SFTP ou autres) ou toute autre utilisation similaire est interdite. Le Cégep se garde le droit de vérifier la bande passante consommée par les personnes utilisatrices du réseau. Toute utilisation abusive pourra être sanctionnée.

4.1.7 Utilisation des plateformes SaaS (Software as a Service)

L'utilisation des plateformes SaaS (logiciels accessibles via Internet) par le personnel du Cégep doit se faire dans le respect des politiques institutionnelles en matière de sécurité de l'information², de confidentialité des données³ et la politique sur la protection des renseignements personnels⁴. Bien que ces outils offrent une flexibilité et une accessibilité accrues, ils peuvent également présenter des risques liés à la protection des renseignements personnels, à la souveraineté des données et à la sécurité des systèmes informatiques. Avant d'adopter ou d'utiliser une solution technologique (logiciel, plateforme, service infonuagique ou SaaS), le personnel doit s'assurer de sa conformité auprès de la direction responsable des ressources informationnelles. Cette dernière est responsable au maintien de la liste des solutions approuvées pour l'établissement et du processus d'analyse pour toute nouvelle demande. Toute utilisation non autorisée ou non conforme pourrait entraîner des conséquences disciplinaires et compromettre la sécurité du parc informatique du Cégep.

4.1.8 Utilisation des outils d'intelligence artificielle

L'utilisation des outils d'intelligence artificielle (IA), qu'ils soient accessibles via des plateformes SaaS ou intégrés aux logiciels institutionnels, doit se faire dans le respect des politiques institutionnelles en vigueur. La Direction des ressources informationnelles est habilitée à émettre des directives encadrant spécifiquement l'utilisation des outils d'IA, notamment en ce qui concerne la protection des renseignements personnels, la confidentialité des données institutionnelles, la fiabilité de l'information générée et les usages pédagogiques et administratifs autorisés. Toute directive ainsi émise s'intègre au présent Règlement et encadre les pratiques de l'ensemble des personnes utilisatrices.

4.2 Accès au réseau du Cégep et à son contenu

4.2.1 Identifiant réseau

Il est de la responsabilité de la personne utilisatrice de préserver la confidentialité de ses identifiants réseau et de la configuration de son authentification à facteurs multiples. Toute personne est responsable des actions effectuées lors de l'accès au réseau effectué à l'aide de son identifiant. Pour cette raison, une

¹ Politique de respect de la personne et de civilité en milieu de vie collégial du Cégep de l'Outaouais

² Politique relative à la sécurité de l'information (DSA-P4)

³ Politique de confidentialité (DG-P5)

⁴ Politique sur la protection des renseignements personnels (DG-P6)

personne utilisatrice ne doit, en aucun cas, communiquer, transmettre ou dévoiler son mot de passe confidentiel à une autre personne.

Pour la même raison, il est interdit à tout membre du personnel du Cégep de demander ou d'exiger toute partie de l'identifiant d'une personne, à moins que cela ne soit expressément nécessaire pour assurer la pérennité ou la qualité des services.

4.2.2 Accès aux laboratoires informatiques

Les locaux servant de laboratoires informatiques sont accessibles uniquement aux personnes autorisées. Le Cégep peut également réserver certains laboratoires pour des activités de formation spécifiques.

Les personnes utilisatrices doivent respecter les horaires d'ouverture, la disponibilité et le caractère spécialisé des laboratoires informatiques.

Afin de protéger l'équipement informatique, il est interdit de boire ou de manger dans les laboratoires informatiques.

4.2.3 Matériel illicite

L'utilisation, l'installation, le téléchargement, la copie, la distribution et le recel de matériel illicite sont interdits. La participation à de tels actes est illégale et le Cégep se réserve le droit, dans de tels cas, d'appliquer des sanctions pouvant s'ajouter aux sanctions pénales prévues par la *Loi*.

Les reproductions de logiciels ne sont autorisées qu'à des fins de copies de sécurité, selon les normes de la licence d'utilisation qui les régissent. Malgré ce qui précède, toute copie doit être autorisée au préalable par la personne administratrice du parc informatique et multimédia et réalisée sous la supervision d'un membre du personnel technique.

4.2.4 Identifiant réseau utilisé

Chaque accès à un ordinateur d'un laboratoire informatique doit être effectué en utilisant l'identifiant réseau propre à la personne utilisatrice. Toute tentative d'usurpation d'identité, délibérée ou non, pourra être passible de sanction.

4.2.5 Protection de l'identifiant réseau

Chaque personne a la responsabilité de protéger les informations de ses identifiants réseaux et celles fournies par l'authentification à facteurs multiples.

À l'inverse, il est strictement interdit de tenter de déchiffrer, de découvrir ou de deviner, par tout moyen informatique ou autre, l'identifiant réseau ou toute partie de l'identifiant réseau d'une personne utilisatrice.

4.2.6 Retrait de l'autorisation d'accès

Sous réserve de toute politique, tout règlement du Cégep ou tout avis émis par la Direction des relations humaines et du développement organisationnel comportant une disposition contraire : lorsque le Cégep retire le droit d'utilisation des équipements informatiques et multimédias, par sanction ou pour toute autre raison que ce soit, les informations, données personnelles et logiciels de la personne utilisatrice seront considérés comme périmés après le délai de rétention configuré sur les logiciels de sauvegarde.

La personne administratrice du parc informatique et multimédia sera alors en droit d'appliquer les pratiques en vigueur quant à la suppression de données périmées, sans autre droit de recours ultérieur par la personne utilisatrice.

4.3 Informations des personnes utilisatrices

4.3.1 Données appartenant à la personne utilisatrice

Dans le cadre de son travail, la personne utilisatrice doit, en toute circonstance, sauvegarder ses données sur le stockage réseau du Cégep ou sur la plateforme Microsoft 365 et non sur le poste de travail lui-même. Toute personne utilisatrice qui sauvegarde des données localement sur un poste de travail informatique reconnaît dès lors, en assumant la responsabilité quant à la protection contre la perte ou la destruction et ne pourra donc invoquer quelque responsabilité du Cégep à cet égard.

Les données qui sont la propriété du Cégep (institutionnelles) doivent être stockées seulement sur le réseau local, OneDrive ou SharePoint. Les espaces de stockage (local et infonuagique) fournis à chaque utilisateur ne doivent pas être utilisés pour stocker des documents personnels confidentiels sans lien avec les fonctions exercées.

À la fin du contrat d'emploi, il est de la responsabilité de l'employé de faire une sauvegarde des données qui lui appartiennent seulement et de ne pas confondre avec des données qui appartiennent à l'organisation.

4.3.2 Fermeture de session sur le poste de travail de la personne utilisatrice

Afin d'assurer la confidentialité des données et de se protéger contre toute action effectuée à l'aide de son identifiant réseau, toute personne utilisatrice a l'obligation de fermer sa session ou de verrouiller son poste de travail lorsqu'elle quitte son bureau ou doit s'absenter.

Nulle personne ayant failli à ces bonnes pratiques pourra invoquer la responsabilité du Cégep advenant l'accès non autorisé à son poste de travail, ou lors de tout acte perpétré à ce moment à partir de son compte, même si la personne peut démontrer qu'elle n'était pas à son poste de travail au moment des faits.

4.3.3 Utilisation partagée d'un poste de travail

Le Cégep reconnaît que plusieurs personnes utilisatrices peuvent parfois partager un même poste de travail. Malgré les bonnes pratiques présentées à l'alinéa 4.3.2, il est donc possible que le poste de travail ne soit pas verrouillé. Le cas échéant, la nouvelle personne utilisatrice doit procéder immédiatement à la fermeture de la session ou redémarrer le poste de travail. L'utilisation inappropriée d'une session d'une autre personne pourra être considérée comme une usurpation d'identité et passible des sanctions appropriées.

4.4 Modification des équipements informatiques

4.4.1 Ajout de logiciel

Sauf dans le cas d'activités pédagogiques encadrées, il est interdit d'ajouter, de retirer ou de modifier tout logiciel sur les équipements informatiques sans l'autorisation préalable de la personne administratrice du parc informatique et multimédia ou d'une personne membre du personnel technique. Les utilisateurs ont la capacité de faire l'installation des logiciels offerts par le Cégep à travers la plateforme de déploiement logiciel « Portail d'entreprise » de Microsoft. Toute application ne se trouvant pas dans ce portail n'a pas été sanctionnée par le Cégep et pourrait être bloquée ou effacée sans préavis.

La personne utilisatrice à qui l'on a attribué un privilège d'administration des éléments logiciels sur son poste de travail doit utiliser ce droit de façon circonspecte. Celle-ci doit signer une entente qui est utilisée pour documenter le besoin et l'inventaire des utilisateurs avec des privilèges d'administration. Elle a le devoir de faire en sorte que les ajouts et les modifications qu'elle effectue à son poste de travail n'altèrent pas les fonctionnalités de celui-ci, surtout en matière de cybersécurité ou par l'installation d'un logiciel qui n'a pas été approuvée par la Direction en charge des ressources informationnelles. En cas d'incident, la responsabilité du Cégep se limite strictement à remettre le poste de travail dans un état fonctionnel, quitte à devoir rétablir la configuration d'origine du poste de travail en cas de besoin.

Tous les équipements informatiques et multimédias fournis par le Cégep bénéficient du soutien informatique nécessaire à leur bon fonctionnement.

4.4.2 Modification matérielle des équipements

Sauf dans le cas d'activités pédagogiques encadrées, il est interdit d'ajouter, de retirer ou de modifier tout élément matériel des équipements informatiques sans l'autorisation préalable de la personne administratrice du parc informatique et multimédia ou d'une personne membre du personnel technique. Dans tous les cas, toute modification matérielle des équipements doit être effectuée par une personne responsable désignée, soit par une personne membre du personnel technique de la Direction en charge des ressources informationnelles.

Pour en assurer la longévité et permettre leur réutilisation dans les meilleures conditions, il est interdit d'apposer des autocollants ou toute autre décoration sur les équipements. Seules les étiquettes d'identification officielles (code à barres ou numéro d'inventaire) sont autorisées. De manière générale, un soin raisonnable est attendu dans la manipulation et l'utilisation des équipements confiés.

4.4.3 Déplacement des équipements

Sauf dans le cas d'activités pédagogiques encadrées, il est interdit de déplacer des équipements informatiques sans l'autorisation préalable de la personne administratrice du parc informatique et multimédia ou d'une personne membre du personnel technique, sauf pour le matériel prévu à cet effet et pour lequel vous êtes autorisés à le faire (ex. portable, chariot de portables, etc.) Tout autre déplacement doit se faire sous la supervision d'une personne responsable désignée par la personne administratrice du parc informatique et multimédia ou d'une personne membre du personnel technique.

4.5 Messagerie électronique

4.5.1 Utilisation de la messagerie électronique

La vocation première du système de courrier électronique est d'appuyer la poursuite de la mission du Cégep de l'Outaouais en tant qu'établissement d'enseignement. Le Cégep en autorise l'usage exceptionnel à des fins privées, à condition que cet usage soit occasionnel, qu'il se déroule à l'extérieur des heures de prestation de travail ou de services, qu'il n'affecte pas la productivité du personnel et qu'il demeure en tout temps conforme aux dispositions du présent *Règlement*.

En faisant usage de ce service à titre personnel, la personne utilisatrice est tenue d'indiquer, dans le sujet du message, que celui-ci a un caractère privé. La signature modèle du Cégep ne doit alors pas apparaître à la fin du message électronique; elle doit être remplacée par une signature personnelle, indiquant clairement qu'il s'agit d'un message personnel et que les faits ou opinions émis dans le message électronique le sont à titre personnel seulement.

Il est strictement interdit d'utiliser le système de courrier électronique en vue :

- d'envoyer des messages pour des fins commerciales, non autorisées ou illégales;
- d'envoyer ou faire suivre (*forward*) des messages électroniques en l'absence de but institutionnel légitime, ou dans des circonstances de nature à porter préjudice au Cégep, à quelque membre de son personnel ou de sa communauté étudiante, ou à l'auteur ou l'auteur du message original;
- d'envoyer des messages dont le contenu est susceptible de porter atteinte à la dignité d'autrui ou au Cégep de l'Outaouais, ou comportant ou liant vers des éléments à caractère érotique ou pornographique, prônant la discrimination sur la base du sexe, de l'orientation sexuelle, du handicap, de la religion, de la race ou de l'origine nationale ou ethnique;
- d'envoyer massivement des messages non sollicités, pratique associée à du pollupostage (*spamming*) sans un appui officiel du Cégep avec des outils prévus à cet effet.

4.5.2 Identité et usurpation

Lors de tout envoi, réponse ou renvoi, la personne utilisatrice doit s'identifier clairement en tant qu'elle-même; en aucun cas elle ne doit usurper ou tenter d'usurper l'identité d'une autre personne.

4.5.3 Qualité de la langue

En tant qu'établissement d'enseignement, le Cégep doit donner l'exemple par la qualité de ses communications. En ce sens, l'orthographe, la syntaxe, la grammaire et le style doivent être soignés et de qualité supérieure. Pour aider son personnel dans cette tâche, le Cégep rend disponibles des outils informatiques de correction.⁵

⁵ Politique relative à l'emploi et à la qualité de la langue française (DG-P2)

4.5.4 Niveau de langue

La personne utilisatrice doit rédiger ses messages électroniques dans un langage courtois. Il est interdit de recourir à un vocabulaire injurieux, malveillant, haineux ou discriminatoire, ou se livrer à toute forme de harcèlement, de menace, d'intimidation ou de diffamation.

4.5.5 Transmission de documents confidentiels

L'article 2088 du *Code civil du Québec* prévoit que toute personne salariée, outre qu'elle soit tenue d'exécuter son travail avec diligence, doit agir avec loyauté et ainsi s'abstenir de collecter, consulter ou faire usage de tout renseignement de nature confidentielle à des fins autres que celles expressément requises par l'exécution de ses tâches.

La personne utilisatrice doit également faire usage de mesures de protection et de sécurité adéquates lors de la transmission de documents ou d'informations de nature confidentielle, notamment des renseignements protégés en vertu de la *Loi sur l'accès à l'information* ou des informations stratégiques.⁶

4.5.6 Utilisation des listes de distribution corporatives

Il est interdit d'utiliser les listes de distribution corporatives sans autorisation préalable des directions des services concernés. Sans égard à ce qui précède, il demeure toutefois interdit d'utiliser ces listes pour des diffusions massives non sollicitées ou abusives, ou pouvant être assimilées à du pollupostage.

4.5.7 Utilisation des listes de distribution personnelles

Il est permis de se créer des listes de distribution personnelles, mais il est interdit d'utiliser ces listes pour des diffusions massives non sollicitées ou abusives, ou pouvant être assimilées à du pollupostage. Les personnes utilisatrices sont invitées à procéder régulièrement à la mise à jour de leurs listes, de telle sorte qu'elles ne contiennent que des membres actifs.

ARTICLE 5 RESPONSABILITÉS DU CÉGEP

5.1 Confidentialité des informations

Le Cégep protège la confidentialité et l'intégrité des messages électroniques, des fichiers et des espaces de sauvegarde dédiés aux différentes personnes sur le réseau. Il protège également la personne utilisatrice contre l'intrusion par des personnes non autorisées sur le réseau du Cégep.

5.2 Sécurité des données sur le réseau

Le Cégep prend des mesures de sauvegarde adéquates pour protéger les documents ou les données déposées sur le réseau par les personnes utilisatrices.

5.3 Protection des systèmes informatiques

Le Cégep instaure des mesures de contrôle et de sécurité appropriées pour protéger adéquatement les équipements informatiques sous sa responsabilité. Il gère ses équipements de manière licite et efficace en respectant le caractère confidentiel de l'information, qu'elle soit en transit ou emmagasinée par les personnes utilisatrices sur les réseaux du Cégep, lors de toute intervention de gestion par l'équipe de la Direction en charge des ressources informationnelles.

5.4 Renseignements protégés

L'information contenue dans les équipements informatiques, de même que sur le réseau, est confidentielle lorsqu'elle a le caractère d'un renseignement nominatif ou le caractère d'un renseignement relatif à la vie privée de la personne au sens du *Code civil du Québec*. Cette information est protégée et n'est accessible que par les personnes mandatées par le Cégep.⁷

⁶ Politique sur la protection des renseignements personnels (DG-P6)

⁷ Politique sur la protection des renseignements personnels (DG-P6)

5.5 Protection contre les logiciels malveillants

Le Cégep vérifie régulièrement et fréquemment l'absence de virus ou de logiciels malveillants (*malware*) dans son parc informatique.

5.6 Vérification

Le personnel en charge de la sécurité informatique, accompagnée d'un membre du personnel d'encadrement, est autorisée à procéder aux vérifications nécessaires des équipements informatiques et systèmes afin de s'assurer du respect des politiques, des règlements, des directives ou des règles d'utilisation du Cégep et des lois ou des règlements provinciaux ou fédéraux en vigueur.

5.7 Droit d'auteur

Conformément à la Loi sur la protection des droits d'auteur, le Cégep, sauf stipulation contraire d'une loi, un règlement ou une convention collective, est le premier titulaire des droits d'auteur de toute œuvre portée sur ses systèmes d'information, incluant tout logiciel, tout matériel transmis à des clavardages en ligne (chat), des forums de discussion (newsgroups), des réseaux sociaux, ou des pages Word Wide Web (www) et des messages électroniques créés par une personne utilisatrice, dans le cadre de son travail.

ARTICLE 6 SANCTIONS

Toute personne qui contrevient à ce *Règlement* est passible de sanctions.

6.1 Restrictions d'utilisation

Le Cégep se réserve, notamment, le droit de retirer l'autorisation d'utilisation des équipements informatiques et d'interdire l'accès à ses équipements à quiconque ne respecte pas le présent *Règlement* ou cause, par une utilisation abusive ou négligente, des dommages aux équipements informatiques ou aux ressources informatiques.

Ce droit ne saurait remplacer ou limiter le droit à tout autre recours, judiciaire ou civil, contre toute personne tenue responsable de gestes révélant une utilisation malveillante, sciemment négligente ou illégale des équipements informatiques du Cégep.

6.2 Sanctions disciplinaires

Le Cégep se réserve le droit d'imposer des sanctions disciplinaires à toute personne salariée ayant eu recours au parc informatique pour contrevenir au principe de loyauté envers l'employeur, incluant mais sans s'y limiter en tenant des propos ou en diffusant des informations dont le contenu est susceptible de porter atteinte à la dignité d'autrui ou de son employeur.

ARTICLE 7 CYBERSÉCURITÉ ET PROTECTION DES DONNÉES

7.1 Formation et sensibilisation

En conformité aux obligations ministérielles, les personnes utilisatrices auront accès à de la sensibilisation et devront maintenir leurs connaissances en suivant le plan de formation en cybersécurité du Cégep de l'Outaouais. Ces formations peuvent également inclure des volets portant sur l'utilisation sécuritaire et éthique des outils d'intelligence artificielle.

7.2 Sécurité d'accès et authentification à facteurs multiples

L'accès aux ressources stratégiques est protégé par un système d'authentification à facteurs multiples (AFM). Les personnes utilisatrices ne doivent en aucun temps partager leur mot de passe et doivent l'utiliser exclusivement pour Microsoft 365 et Omnivox du Cégep.

7.3 Mise à jour et gestion des vulnérabilités

Tous les équipements et logiciels utilisés dans l'environnement du Cégep doivent bénéficier de mises à jour régulières et de correctifs de sécurité. Il est sous la responsabilité de la personne utilisatrice de permettre à l'équipement de faire les mises à jour proposées par celui-ci en respectant les délais indiqués par l'équipement.

7.4 Chiffrement et protection des échanges

Les données sensibles, qu'elles soient stockées ou en transit, doivent être protégées par des mécanismes de chiffrement conformes aux normes en vigueur (ex. : TLS/SSL pour les communications). Tout partage d'information, de documents et de données doit respecter la Politique sur la protection des renseignements personnels du Cégep⁸.

7.5 Surveillance et détection des incidents

Le Cégep met en place des outils de surveillance en continu pour détecter rapidement toute activité anormale, tentative d'intrusion ou menace. Des audits de sécurité et des tests d'intrusion réguliers sont réalisés pour évaluer la robustesse des systèmes. Tout incident de sécurité confirmé ou suspecté doit être signalé par le guichet unique. Afin de ne pas compromettre nos systèmes, l'enquête ou la résolution de l'incident, les personnes impliquées doivent préserver la confidentialité des informations s'y rapportant. L'équipe de sécurité peut exiger la collaboration des personnes impliquées et assurera les suivis requis selon l'évolution de la situation.

ARTICLE 8 APPLICATION DU RÈGLEMENT

La Direction des ressources informatiques et multimédias est responsable de l'application de ce *Règlement*. En plus de veiller à l'application des règles d'utilisation, la personne responsable du *Règlement* est chargée de la sensibilisation des différentes personnes utilisatrices du Cégep au regard des comportements attendus. À titre d'exemple, et sans s'y limiter, ces moyens de sensibilisation pourraient inclure la préparation d'affiches pour informer le personnel sur les bonnes pratiques attendues.

ARTICLE 9 PARTAGE DES RESPONSABILITÉS

Les gestionnaires s'assurent du respect de l'application du *Règlement relatif à l'utilisation du parc informatique et multimédia* au sein du personnel qu'elles ou qu'ils regroupent.

ARTICLE 10 ENTRÉE EN VIGUEUR

Le présent *Règlement* entre en vigueur au moment de son acceptation par le conseil d'administration du Cégep.

ARTICLE 11 RÉVISION DU RÈGLEMENT

La révision du présent *Règlement* est prévue deux ans après son entrée en vigueur.

⁸ Politique sur la protection des renseignements personnels (DG-P6)