

DIRECTIVES ET PROCÉDURES

DIRECTIVES ET PROCÉDURES ADMINISTRATIVES	DE NATURE ADMINISTRATIVE
TITRE :	UTILISATION DE L'INFRASTRUCTURE TECHNOLOGIQUE
CODE NUMÉRIQUE :	ADM-10
RESPONSABLE DE LA DIFFUSION :	Chef des Technologies et de l'expérience numérique
GROUPES ou SECTEURS CONSULTÉS :	Direction des ressources physiques
ENTRÉE EN VIGUEUR :	29 août 2012
DERNIÈRE RÉVISION :	4 mars 2020
FRÉQUENCE DE RÉVISION	Cette directive est révisée et validée tous les 5 ans

Dans le présent document, le genre masculin est utilisé afin d'alléger le texte et se veut inclusif et utilisé autant pour désigner les femmes, les hommes et le genre neutre.

1. OBJECTIFS

Veiller à ce que tout utilisateur autorisé qui accède et utilise l'infrastructure technologique du Collège évite de compromettre la sécurité des systèmes.

Communiquer clairement les attentes du Collège concernant l'utilisation de l'infrastructure technologique afin de veiller à ce que tout utilisateur adopte un comportement dont la conduite de ses activités et la transmission de renseignements le rendent imputable s'il pratique des comportements interdits, illégaux, inappropriés ou qui pourraient avoir des répercussions négatives sur La Cité.

2. ÉNONCÉ

Le Collège s'engage à miser sur l'excellence et l'amélioration continue quant aux services et développements technologiques. Il encourage tout utilisateur autorisé à travailler de façon professionnelle, éthique et licite lorsqu'il utilise l'infrastructure technologique mise à sa disposition dans le cadre de la mission du Collège et dans le but d'augmenter l'efficacité organisationnelle et la prestation des services.

3. DESTINATAIRES

La directive s'applique à tout utilisateur autorisé ayant accès à l'infrastructure technologique du Collège, dans les locaux du Collège ou à distance.

La directive concerne l'ensemble de l'infrastructure technologique du Collège, les services hébergés (tels que live@edu et Adobe Connect) ainsi que tous les comptes utilisateurs utilisés par la communauté collégiale tant ceux dont l'accès est assuré par de l'équipement fourni par le Collège que ceux qui appartiennent aux utilisateurs autorisés.

4. DÉFINITIONS

Le terme « utilisateur autorisé » fait référence à toute personne qui a obtenu l'autorisation du Collège pour accéder à son infrastructure technologique et à l'utiliser et fait référence à tout étudiant inscrit, à temps plein ou à temps partiel, à tous les employés du Collège, tous les employés des services associés, tous les membres du Conseil d'administration, tous les membres des divers comités, à tous les bénévoles et visiteurs à qui un responsable autorisé par le Collège a accordé un statut d'utilisateur.

Le terme « infrastructure technologique » fait référence à l'ensemble des ordinateurs, des appareils périphériques, des systèmes de courriel, de boîte vocale et de messagerie instantanée, des logiciels, des appareils sans fil (p. ex. : téléphones portables ou intelligents), des réseaux et des systèmes électroniques ainsi que des renseignements, des données ou des fichiers qui y sont archivés.

5. PRINCIPES GÉNÉRAUX

Toutes les composantes de l'infrastructure technologique demeurent la propriété du Collège en tout temps et doivent être remises au Collège sur demande.

L'utilisateur autorisé est responsable de toute activité associée à son identité et à son mot de passe et doit exercer son bon jugement dans l'usage de l'infrastructure technologique. Toute forme d'usage abusif ou inapproprié de l'infrastructure technologique pourrait avoir des conséquences directes sur l'utilisateur fautif.

L'utilisateur autorisé doit savoir que les renseignements archivés ou transmis dans l'infrastructure technologique peuvent être divulgués à des tiers, notamment en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels ou faire l'objet d'un suivi conformément aux modalités prévues dans la présente directive ou toute autre directive du Collège.

L'utilisateur autorisé doit savoir que certaines des ressources du réseau du Collège sont fournies par des tiers, qui peuvent être situés aux États-Unis ou autres juridictions. En utilisant les réseaux du Collège, l'utilisateur reconnaît et comprend que les contenus et renseignements affichés, reçus ou envoyés au moyen des réseaux du Collège peuvent être logés dans des systèmes situés aux États-Unis ou autres juridictions; ils peuvent donc être soumis à la loi américaine Patriot Act ou autres lois applicables qui peut exiger du Collège la divulgation de contenu.

Le Collège surveille et analyse l'utilisation de l'infrastructure technologique afin de maintenir et d'assurer l'efficacité du fonctionnement et d'assurer une conformité avec les directives institutionnelles et les lois applicables. Si le Collège a des motifs de croire qu'un utilisateur autorisé fait un usage non conforme ou abusif de l'infrastructure technologique, une enquête pourra être menée et pourra comprendre une surveillance spéciale de l'utilisation des systèmes, de la lecture du contenu de courriels ou de fichiers électroniques.

L'utilisateur reconnaît et comprend qu'à l'occasion, les réseaux et systèmes du Collège et les équipements raccordés aux réseaux peuvent tomber en panne de façon inattendue. Par conséquent, le Collège et ses fournisseurs de services ne sont en aucune façon responsables des pertes de temps ou de données causées par ces interruptions involontaires.

6. VIE PRIVÉE ET CONFIDENTIALITÉ DES DONNÉES

Le Collège respecte la vie privée des utilisateurs autorisés. Toutefois, du fait que l'ensemble de l'infrastructure technologique est la propriété exclusive du Collège et est fourni à des fins pédagogiques ou professionnelles, l'atteinte à la vie privée de l'utilisateur autorisé ne s'étend pas à l'utilisation des systèmes de communication électronique ou aux messages envoyés ou reçus par ces systèmes.

L'utilisateur autorisé ne doit pas s'attendre à ce que toutes les informations emmagasinées dans l'infrastructure technologique (ordinateurs, boîte vocale ou tout autre équipement électronique, peu importe que l'information soit contenue sur disque dur ou sur tout autre support) soient privées. Le Collège ne contrôle pas systématiquement les communications des utilisateurs autorisés. Un contrôle aura lieu s'il a des raisons de croire que les systèmes sont utilisés de façon inappropriée ou s'il y a un risque de sécurité associé au traitement de l'information.

Les systèmes appartiennent ou sont enregistrés au nom du Collège et, par conséquent, sont accessibles en tout temps par le personnel autorisé du Collège ou pour toute autre raison légale ou d'affaires telles que spécifiées ci-après. Les mots de passe donnant accès à l'infrastructure technologique servent à protéger les systèmes du Collège et non pas à assurer la vie privée de l'utilisateur autorisé.

Pour répondre à toute procédure judiciaire qui exigerait la production de preuves ou de documents emmagasinés sur des supports d'information, le Collège doit être en mesure de retracer des fichiers et des documents. Des copies d'archivage et de sauvegarde des messages électroniques peuvent exister, malgré la suppression des droits d'accès de l'utilisateur, en conformité avec la directive de conservation des dossiers. Les objectifs de ces procédures de sauvegarde et d'archivage sont d'assurer la fiabilité des systèmes, de prévenir la perte de données corporatives, de répondre aux obligations légales.

En naviguant sur Internet et le Web, l'utilisateur doit être conscient qu'un logiciel de filtrage journalise l'ensemble des sites visités et que le Collège, au besoin, peut consulter ce journal afin d'assurer un usage adéquat d'Internet. Cette journalisation fonctionne sur une base continue et sans interruption et le Collège peut restreindre l'accès à un site ou une catégorie de sites à sa discrétion.

7. MODALITÉS D'UTILISATION

a. USAGE PROFESSIONNEL OU PÉDAGOGIQUE

L'utilisateur autorisé est responsable d'exercer son bon jugement dans l'usage de l'infrastructure technologique. L'utilisateur peut accéder au réseau et aux systèmes technologiques dans le cadre d'activités professionnelles ou pédagogiques. L'utilisation de l'infrastructure technologique, d'Internet et des médias sociaux, par l'utilisateur autorisé, doit se faire dans le respect des directives institutionnelles, et ce, sans porter atteinte à des personnes ou à la réputation du Collège.

b. USAGE PERSONNEL

Le Collège reconnaît que l'utilisateur autorisé peut avoir besoin, à l'occasion, d'utiliser l'infrastructure technologique à des fins personnelles. Cette utilisation est acceptable si elle respecte les critères suivants :

- se limite aux temps libres (ex. pauses)
- respecte les lois, normes de conduite, directives institutionnelles, pédagogiques et autres
- préserve l'intégrité et le bon fonctionnement des systèmes
- évite de perturber le lieu de travail
- évite de nuire à la réputation du Collège et à lui refiler la responsabilité
- évite d'entraîner des frais pour le Collège
- ne vise pas des gains personnels

c. USAGE À DISTANCE

L'utilisateur autorisé qui se sert de l'infrastructure technologique du Collège à l'extérieur de l'organisation doit assurer la même vigilance que lorsqu'il est au Collège et doit respecter les mêmes règles d'utilisation et de sécurité.

d. USAGE INACCEPTABLE OU INAPPROPRIÉ

En aucun temps, l'infrastructure technologique du Collège ne doit servir à commettre une action illégale aux yeux de la loi, à cautionner des agissements inacceptables d'un point de vue moral ou à contourner les directives du Collège. Toute activité qui semble répréhensible doit être signalée à l'autorité pertinente du Collège. Les utilisations inacceptables peuvent aussi être une infraction au Code criminel du Canada et faire l'objet de poursuites dans certains cas. Les exemples suivants sont énoncés à titre indicatif et ne sont pas limitatifs :

- Désactiver ou tenter de désactiver les dispositifs de sécurité des systèmes et services du Collège
- Présenter des opinions personnelles comme étant celles du Collège
- Fournir des renseignements qui portent atteinte à la crédibilité du Collège
- Mettre les équipements à la disposition des personnes non autorisées
- Accéder à des sites de rencontres, des sites d'échanges, des blogues ou à toute autre forme ou catégorie de sites qui peuvent entacher la réputation du Collège
- Envoyer ou télécharger des types d'affichage comme :
 - des messages, images ou blagues à connotation sexuelle ou érotique
 - des propositions malvenues, des demandes de rendez-vous ou des lettres d'amour
 - des injures à connotations ethniques, raciales ou religieuses
 - tout autre message, image, blague ou dessin qui peut constituer du harcèlement, du dénigrement ou autre forme de discrimination fondée sur des motifs prohibés par le Code des droits de la personne

- Effectuer toute action qui constitue de la falsification électronique (p. ex. : usurpation d'identité)
- Héberger, sur les réseaux, des équipements agissant à titre de serveur sans permission explicite de secteur des Technologies de l'information

e. USAGE ILLICITE

Toute activité qui enfreint une loi ou un règlement ou qui rend un utilisateur autorisé du Collège passible de poursuites est strictement interdite. Les exemples suivants sont énoncés à titre indicatif et ne sont pas limitatifs :

- Divulguer, sans autorisation préalable, des renseignements institutionnels à diffusion restreinte et confidentielle
- Violer des droits de propriété intellectuelle en reproduisant, en distribuant ou en utilisant des documents ou renseignements protégés par des droits d'auteur, une marque de commerce ou une convention de droit d'utilisation
- Propager une fausse allégation susceptible de nuire à la réputation d'une personne
- Intercepter ou lire le courrier électronique d'un autre utilisateur ou d'autres renseignements privés sans avoir l'autorisation
- Détruire, modifier, falsifier ou crypter des données ou des dossiers électroniques sans autorisation et dans l'intention d'en réduire l'accès à des personnes autorisées
- Obtenir un accès non autorisé à l'infrastructure technologique en utilisant le mot de passe, l'identité d'un autre utilisateur dans le but de commettre une fraude ou d'obtenir des biens ou des services
- Nuire à l'intégrité des systèmes technologiques de façon intentionnelle par divers moyens de propagation (p. ex. : virus)
- Posséder, télécharger, stocker, afficher ou distribuer du matériel frauduleux, sexuellement explicite, blasphématoire, obscène, intimidant, harcelant ou autrement illicite ou qui fait la promotion de la violence

8. SÉCURITÉ

a. ACTIVATION ET MOT DE PASSE DE L'UTILISATEUR

L'accès aux systèmes est contrôlé par des comptes individuels et des mots de passe. Tous les utilisateurs autorisés, à l'exception des bénévoles et des visiteurs, reçoivent un compte utilisateur individuel. Celui-ci est créé dans les 24 heures suivant l'inscription, pour les étudiants, et suivant l'embauche pour les autres utilisateurs. La résiliation du compte se fait à la fin des études et à la fin de l'embauche. Le Collège se réserve toutefois le droit de suspendre temporairement ou de terminer l'accès au compte d'un utilisateur autorisé qui ne se conforme pas aux politiques, directives administratives et pédagogiques et toutes autres lois applicables. Toute violation des lois applicables peut également être signalée au corps policier approprié.

L'utilisateur autorisé doit éviter de divulguer son mot de passe à quiconque de manière à éviter de lui permettre d'accéder à l'infrastructure technologique. Lors de l'absence d'un utilisateur autorisé, le secteur des Technologies de l'information est responsable de fournir un mot de passe au remplaçant. Si des informations pertinentes doivent être extraites du système d'un utilisateur absent, le secteur des Technologies de l'information fera l'extraction à l'aide de méthodes sécuritaires.

b. SYSTÈMES ET INFORMATIONS CORPORATIVES

Si des informations stratégiques ou institutionnelles du Collège sont perdues, divulguées à des parties non autorisées ou si le Collège soupçonne qu'elles ont été perdues ou divulguées à des parties non autorisées, l'utilisateur autorisé doit informer immédiatement le secteur des Technologies de l'information. De la même façon, si des logiciels ou des applications présentent un fait étrange ou si un accès non autorisé aux systèmes d'information du Collège a eu lieu ou que le Collège soupçonne qu'un tel accès a eu lieu, le secteur des Technologies de l'information doit en être avisé immédiatement.

c. PROTECTION DES ÉQUIPEMENTS

L'utilisateur autorisé doit protéger les biens technologiques contre l'endommagement accidentel, le vol, la perte ou les risques environnementaux.

9. RESPONSABILITÉ

a. RESPONSABILITÉS DES UTILISATEURS

Les utilisateurs autorisés ont, de façon non limitative, les responsabilités suivantes :

- prendre connaissance de la directive
- utiliser et protéger l'infrastructure technologique du Collège dans le respect de la présente directive et de toute autre procédure du Collège
- prendre toutes les mesures raisonnables afin de protéger l'utilisation des comptes protégés par des mots de passe attribués ou choisis, les noms d'utilisateur et autres moyens d'authentification et de contrôle
- signaler à leur superviseur, professeur ou toute autre personne en autorité s'ils constatent ou soupçonnent une infraction à la directive ou à la sécurité de l'infrastructure technologique
- consulter uniquement les fichiers et les données auxquelles ils ont accès et qui sont nécessaires à leurs études ou à leur travail
- participer aux enquêtes qui pourraient être menées par des représentants autorisés par le Collège

b. RESPONSABILITÉS DES SUPERVISEURS ET DU PERSONNEL PÉDAGOGIQUE

Les superviseurs immédiats et le personnel pédagogique ont, de façon non limitative, les responsabilités suivantes :

- veiller à ce que les utilisateurs autorisés connaissent et respectent la directive
- signaler et faire rapport lors d'activités inacceptables, illicites ou qui sont contraires aux directives du Collège
- signaler, selon la procédure en vigueur, aux utilisateurs qui quittent le Collège la révocation de leurs droits d'accès aux systèmes

c. RESPONSABILITÉS DU SECTEUR DES TECHNOLOGIES DE L'INFORMATION

Le personnel autorisé du secteur des Technologies de l'information a, de façon non limitative, les responsabilités suivantes :

- diffuser et rendre accessible la présente directive aux utilisateurs autorisés
- veiller à l'application de la directive
- organiser, gérer, maintenir et surveiller l'infrastructure technologique dans le respect des responsabilités et droits qui lui sont conférés

- élaborer et réviser les directives nécessaires au bon fonctionnement du Collège
-

10. ENQUÊTE ET DISCIPLINE

Un usage non conforme ou abusif de l'infrastructure technologique peut entraîner, pour un utilisateur autorisé, l'application de mesure administrative ou disciplinaire jugée appropriée et pouvant aller jusqu'à l'expulsion du Collège ou à la rupture du lien d'emploi.

Le Collège se réserve le droit d'enquêter sur toute allégation d'acte répréhensible ou de communiquer tout cas d'acte illicite aux autorités policières compétentes.

11. RÉVISION DE LA DIRECTIVE

Le Collège se réserve le droit de réviser ou de modifier la présente directive, lorsque jugé nécessaire, et ce, sans préavis.
