

COLLÈGE O'SULLIVAN DE QUÉBEC

POLITIQUE D'UTILISATION DES SYSTÈMES ÉLECTRONIQUES ET DES MÉDIAS SOCIAUX

PRÉAMBULE

La présente politique a pour objectif principal de régir l'utilisation des différents systèmes électroniques à des fins de communication. Elle prohibe également certains usages des systèmes électroniques qui sont incompatibles avec la mission du Collège O'Sullivan de Québec, ci-après nommé le Collège.

Cette politique vise à établir les règles du Collège concernant l'utilisation de ses systèmes électroniques, incluant sans limitation:

- le courrier électronique;
- les ordinateurs et équipements qui leur sont reliés;
- le réseau Internet;
- le réseau Intranet;
- les réseaux sociaux;
- l'usage de l'information conservée, communiquée ou traitée par lesdits systèmes;
- encadrer l'échange de messages électroniques (Hotmail, Gmail, textos, Messenger, etc.).

1. ÉNONCÉ

Tous les étudiants qui utilisent ou ont accès aux systèmes électroniques du Collège, et qui utilisent les messages électroniques de quelque provenance qu'ils soient, acceptent de respecter les règles établies dans la présente politique.

2. OBJECTIFS

- Assurer une utilisation sécuritaire des systèmes électroniques du Collège.
- Empêcher l'utilisation inappropriée des systèmes électroniques du Collège.
- Promouvoir le respect des règles régissant la confidentialité de l'information.
- Promouvoir les règles de netiquette sur le Web.

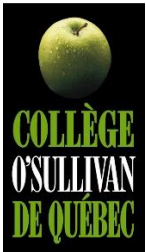
3. CONTENU

3.1 Droit de propriété

Le Collège est propriétaire de toute information ou message créé, envoyé, reçu, mémorisé ou accessible par ses systèmes électroniques dans le cadre des fonctions des utilisateurs. Le Collège détient le droit de vérifier ou de détruire toute information ou tout message non conforme à la présente politique.

3.2 Restrictions quant au contenu des messages

3.2.1 Les communications effectuées au moyen des systèmes électroniques du Collège ne doivent pas être à caractère diffamant, offensant, harcelant, désobligeant ou perturbant et, sans restreindre la généralité de ce qui précède, ne doivent pas contenir des images ou des commentaires à connotation sexuelle, des injures raciales ou toute autre image ou commentaire basé sur l'âge, la race, la couleur, le sexe, la



grossesse, l'orientation sexuelle, l'état civil, la religion, les convictions politiques, la langue, l'origine ethnique ou nationale, la condition sociale ou le handicap.

- 3.2.2 Toutes communications électroniques provenant de systèmes électroniques externes au collège et s'adressant à un autre étudiant du collège ou à un membre du personnel, portant sur les sujets ci-haut mentionnés, qui peuvent porter atteinte à l'intégrité ou à la sécurité de la personne visée, sont strictement interdits.

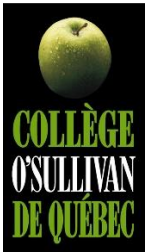
3.3 Activités prohibées

Tout utilisateur des systèmes électroniques du Collège ne peut se servir de ces derniers de manière à compromettre la réputation du Collège, ou pour atteinte à l'intégrité ou à la sécurité d'un tiers, par exemple :

- utiliser une copie illicite d'un logiciel;
- tenter d'infiltrer d'autres ordinateurs;
- détenir, distribuer, visionner ou échanger du matériel pornographique, obscène ou haineux (incluant les écrans de veille et d'arrière-plan);
- se livrer à toute autre activité illégale.

3.4 Un étudiant ne peut employer les systèmes électroniques du Collège pour:

- créer ou distribuer des chaînes de lettres non connexes aux activités du Collège (incluant le publipostage électronique);
- exprimer des opinions à des fins de propagande politique ou religieuse en laissant croire qu'elles émanent du Collège;
- faire de la sollicitation non connexe aux activités pédagogiques du Collège;
- envoyer de la publicité non connexe aux activités pédagogiques du Collège;
- participer à des jeux de hasard ou des paris;
- s'abonner à des listes d'envoi non reliées aux activités pédagogiques du Collège;
- travailler au noir;
- télécharger, transmettre ou distribuer illicitement du matériel breveté ou protégé par les droits d'auteur ou les marques de commerce;
- télécharger, transmettre ou distribuer toute information et tout document confidentiels ou privés sans l'autorisation préalable du Collège ou toute autre autorisation préalable;
- accéder, sans autorisation, à des ordinateurs ou autres systèmes, endommager, altérer ou perturber ces ordinateurs ou systèmes de quelque façon que ce soit;
- utiliser le code d'utilisateur ou le mot de passe d'un autre ou divulguer quelque code ou mot de passe, y compris le sien à moins d'y être dûment autorisé;
- permettre, sans autorisation, à un tiers d'accéder ou d'utiliser les systèmes électroniques du Collège (y compris de fournir accès à de l'information confidentielle à des personnes qui n'y ont pas droit) ou autrement compromettre la sécurité de ses systèmes électroniques ou d'utiliser les systèmes électroniques pour un tiers;
- ouvrir, sans autorisation, du courrier électronique qui ne lui est pas adressé ;
- faire usage de subterfuges ou de moyens pour transmettre du courrier électronique de façon anonyme dans le but d'usurper l'identité d'un usager ou en masquant sa propre identité;
- faire usage du courriel pour tricherie;
- créer des liens de télécommunication à moins d'y être dûment autorisé.



3.5 Garantie de confidentialité

Les communications sur les systèmes électroniques ne sont pas privées et leur sécurité ne peut être assurée. Les mots de passe et les codes d'utilisateur sont octroyés dans le but de protéger l'information confidentielle du Collège contre les tiers et non pas pour conférer un traitement confidentiel aux messages.

- En naviguant sur le réseau Internet, l'étudiant doit se rappeler qu'il peut y avoir un contrôle et une compilation des sites visités.
- L'étudiant doit présumer que toute communication – qu'elle soit personnelle ou non – qu'il crée, envoie, reçoit ou mémorise sur les systèmes électroniques du Collège peut être lue ou entendue par quelqu'un d'autre que le destinataire.
- Afin d'assurer au Collège un accès continu aux informations contenues dans ses systèmes électroniques, l'étudiant ne doit pas se servir de logiciels personnels ou tout autres logiciels non supportés par le Collège pour crypter leur courrier électronique, ou toute autre information contenue ou transmise par les systèmes électroniques du Collège.

3.6 Droit du Collège de surveiller les messages

Le Collège se réserve le droit de surveiller, d'accéder, de récupérer, de lire et de dévoiler les communications dans certaines circonstances, lorsque :

- ses intérêts l'exigent et qu'il est légitime de le faire;
- il a des motifs raisonnables de croire qu'un étudiant se comporte ou est sur le point de se comporter de manière inappropriée en relation avec les systèmes électroniques du Collège;
- il doit examiner le contenu des messages pour obtenir de l'information qui n'est pas autrement disponible;
- il est requis de le faire par la loi ou par une ordonnance de la Cour, lorsqu'il croit raisonnablement qu'un utilisateur a commis, ou est sur le point de poser un geste ou de commettre un acte qui pourrait lui nuire directement ou indirectement;
- l'utilisateur n'est pas disponible (pour cause de maladie, de décès);

3.7 Protection de l'information

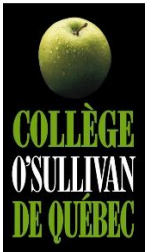
Les messages peuvent facilement être interceptés sur le réseau Internet. L'étudiant doit rapidement voir à éliminer tout message qu'il ne désire pas conserver. De même, le Collège verra au départ de tout étudiant à détruire tout document de nature confidentielle (boîte de courriels et répertoire personnel) qui n'aura pas été physiquement supprimé du support magnétique de l'ordinateur. Le collège verra également à fermer les différents accès aux différents systèmes (Moodle, courriels, répertoire)

3.8 Contravention

Toute contravention à la présente politique, y compris toute infraction aux règles concernant la confidentialité et la sécurité, peut mener à la suspension de privilèges d'accès aux systèmes électroniques du Collège, à la prise de mesures disciplinaires, au remboursement de frais inhérents ou au renvoi de l'étudiant.

3.9 Archivage des fichiers

Tout comme les documents créés, reçus et classés par un utilisateur dans un dossier physique, il est de la responsabilité de chaque étudiant de s'assurer que tous les documents reçus sous support électronique, qui doivent



être conservés, soient sauvegardés conformément aux règles établies par le Collège concernant l'archivage des fichiers. Les messages qui n'ont pas à être sauvegardés doivent être éliminés.

3.10 Virus et altérations illicites

Tout fichier téléchargé à partir du réseau Internet ou tout support informatique amovible doit être balayé par un logiciel antivirus avant son utilisation. Il est expressément interdit d'introduire délibérément des virus, de tenter de percer les systèmes de sécurité ou de procéder à des altérations illicites à l'aide des systèmes électroniques du Collège.

L'étudiant ne doit pas désactiver les systèmes de sécurité mis en place ou tenter de contourner les mécanismes de sécurité en place. L'étudiant doit rapporter immédiatement l'existence de tout virus, de toute altération illicite et de toute autre infraction au responsable du service informatique de son campus.

3.11 Engagement

Tout étudiant s'engage à respecter les termes de la présente politique.

4. RÔLES ET RESPONSABILITÉS

4.1 La Direction générale

- S'assure de l'application de la présente politique.
- S'assure que les privilèges d'accès aux systèmes électroniques sont suspendus lorsque nécessaire.
- Se réserve le droit de mandater, si nécessaire, tout intervenant habilité à exercer une surveillance pertinente sur les systèmes électroniques.
- Est responsable des documents afférents et du respect des lois et règlements concernés par l'application de cette politique.
- Veille à la protection de l'information.

4.2 Le Service des ressources informatiques

- Agit à titre d'administrateur du réseau informatique et, sur demande, peut suspendre les privilèges d'accès aux systèmes électroniques.
- Peut effectuer la surveillance prévue sur demande spécifique de son personnel enseignant ou de la direction du Collège.
- Prend les mesures adéquates afin que les usagers puissent travailler dans un environnement garantissant la sécurité et la confidentialité des informations.
- S'assure de la mise à jour et de l'état de fonctionnement sécuritaire des systèmes électroniques sous leur responsabilité.