

POLITIQUE ET PROCÉDURE

TITRE : Utilisation des équipements et des ressources informatiques		Code :
DESTINATAIRE : Tout le personnel		En vigueur le : 28 juin 2006
ORIGINE : Direction générale	Sanctionné par le c.a. le : 28 juin 2006	Révisé le :

1. PRÉAMBULE

L'office reconnaît l'importance pour ses employés d'avoir accès à ses équipements et ressources informatiques et de télécommunication ainsi qu'au réseau Internet. Par conséquent, il leur accorde ce privilège pour la réalisation d'activités d'apprentissage, de recherche, de gestion, d'administration et de services à la clientèle reliées à la réalisation de la mission de l'office.

En tant que propriétaire et gestionnaire d'équipements et de ressources informatiques, l'office doit s'assurer que leur utilisation et le traitement de l'information ainsi que l'utilisation du réseau Internet soient conformes à certaines normes.

Au delà des dispositions contenues dans la présente politique, l'office s'attend à ce que la conduite de chaque employé soit dictée par les règles usuelles d'éthique, de déontologie et de courtoisie.

Cette politique établit les conditions d'utilisation des équipements et des ressources informatiques par les employés. Elle vise à protéger les investissements collectifs et les employés eux-mêmes contre une utilisation abusive ou illégale des équipements. Elle ne doit donc pas être considéré comme une initiative visant à censurer les membres du personnel.

2. CONSIDÉRATIONS GÉNÉRALES

2.1 Privilège

L'accès aux équipements et aux ressources informatiques constitue un privilège.

Seuls les employés dûment autorisés peuvent avoir accès et utiliser les équipements et les ressources informatiques ou le réseau Internet et ce, dans les limites de l'autorisation accordée aux employés par l'office.

L'utilisation de ce privilège doit être raisonnable et efficace.

2.2 Mise en garde

L'employé qui contrevient aux dispositions de cette politique ou aux directives, règles d'utilisation, s'expose au retrait immédiat de ce privilège, à l'imposition d'une ou de plusieurs des sanctions énumérées à l'article 7.

De plus, l'employé qui commet un acte illégal s'expose à une poursuite judiciaire et à une réclamation de dommages.

2.3 Usage à des fins personnelles

Les employés peuvent faire usage occasionnellement de certains équipements et certaines ressources informatiques de l'office et du réseau Internet aux fins de leur vie privée, par exemple, pour le traitement d'informations qui leur sont personnelles et qui ont un caractère confidentiel, qu'il s'agisse de messages téléphoniques, de courrier électronique ou de

POLITIQUE ET PROCÉDURE

TITRE : Utilisation des équipements et des ressources informatiques
--

traitements informatiques. Cette utilisation ne doit entraver en aucune façon les responsabilités qui leur sont dévolues.

2.4 Usage interdit

Toute utilisation des équipements et des ressources informatiques ainsi que du réseau Internet à des fins non autorisées, illégales ou commerciales ou de publicité, de promotion ou de sollicitation commerciale est strictement interdite.

Est aussi interdite le *clavardage* et l'utilisation de jeux électroniques avec les équipements et les ressources informatiques.

2.5 Modification ou destruction

Toute modification ou destruction des équipements et des ressources informatiques est interdite sans l'autorisation écrite de l'office.

2.6 Actes nuisibles

Il est strictement interdit de poser tout acte pouvant nuire au bon fonctionnement des équipements et des ressources informatiques.

2.7 Utilisation raisonnable

Dans un contexte de partage équitable des ressources, l'employé ne doit pas monopoliser ou abuser des équipements et des ressources informatiques ou du réseau, entre autres, en effectuant un stockage ou un transfert abusif d'informations.

3. CODE D'ACCÈS

3.1 Usage strictement personnel

Un code d'accès individuel est alloué à l'employé par l'office à titre strictement personnel et confidentiel. Il en est de même pour le mot de passe.

3.2 Responsabilité de l'utilisateur

L'employé a un devoir de vigilance et est en tout temps responsable de toute forme de communication effectuée grâce à l'utilisation de son code d'accès ou de son mot de passe et il doit voir à les protéger.

De plus, l'employé est responsable de la protection des données utiles à son travail et de l'accès à celles-ci en s'assurant de les conserver sur le disque du serveur.

3.3 Comportements interdits

Un employé ne peut, en aucun cas, communiquer, transmettre ou dévoiler son code d'accès ou son mot de passe à un autre employé ou à un tiers.

Il est strictement interdit de tenter de décrypter ou de découvrir le code d'accès ou le mot de passe d'un autre employé ou de celui d'un tiers à l'exception du supérieur immédiat.

Dans toute communication, l'employé doit s'identifier selon son code d'accès et en aucun cas il ne doit usurper ou tenter d'usurper l'identité d'un autre employé.

POLITIQUE ET PROCÉDURE

TITRE : Utilisation des équipements et des ressources informatiques

L'absence des restrictions d'accès à des données n'implique pas nécessairement pour un employé le droit de les consulter. Entre autres, l'employé doit s'abstenir de consulter les données affichées ou disponibles à partir d'un poste de travail laissé sans surveillance par son utilisateur, de consulter ou de copier des informations ou des données laissées sans surveillance ou disponibles sans code d'accès ou de mot de passe, à moins qu'il ne soit apparent que l'information est disponible à la catégorie d'utilisateurs dont fait partie l'employé.

4. DROITS DE PROPRIÉTÉ INTELLECTUELLE

4.1 Règle générale

En tout temps, l'employé doit respecter les droits de propriété intellectuelle, notamment les droits d'auteur des tiers.

4.2 Logiciels et progiciels

Les reproductions de logiciels et de progiciels ne sont autorisées qu'à des fins de copies de sécurité ou selon les normes de la licence d'utilisation les régissant.

4.3 Comportements interdits

Il est strictement interdit aux employés :

- d'utiliser toute reproduction illicite d'un logiciel ou d'un fichier électronique; • de participer directement ou indirectement à la reproduction illicite d'un logiciel ou d'un fichier électronique;
- de modifier ou détruire un logiciel, une banque de données ou un fichier électronique, ou d'y accéder sans l'autorisation de son propriétaire; de reproduire la documentation associée à un logiciel sans l'autorisation écrite du titulaire du droit d'auteur de ce logiciel;
- d'utiliser les équipements et les ressources informatiques ou le réseau Internet afin de commettre ou de tenter de commettre une infraction aux lois régissant la propriété intellectuelle.

5. MESSAGERIE ÉLECTRONIQUE, RÉSEAU INTERNET

5.1 Identification

Pour tout message électronique diffusé sur le réseau téléphonique et Internet, l'employé doit s'identifier à titre de signataire de son message et préciser, s'il y a lieu, à quel titre il s'exprime.

5.2 Comportements interdits

Il est strictement interdit aux employés :

- d'utiliser, dans un forum de discussion, dans tout message électronique diffusé sur le réseau ou dans tout message laissé dans une boîte vocale, un message injurieux, malveillant, haineux ou discriminatoire, ainsi que toute forme de harcèlement, de menace ou de diffamation;
- de capter, de stocker, de reproduire ou de transmettre au moyen du réseau Internet ou d'une boîte vocale du matériel ou un message à caractère obscène ou pornographique;
- de procéder au décryptage ou décodage de codes ou de clés d'accès, de fichiers ou de mots de passe, pour quelque raison que ce soit;
- d'utiliser un ou des subterfuges ou d'autres moyens pour transmettre du courrier électronique de façon anonyme ou au nom d'une autre personne.

POLITIQUE ET PROCÉDURE

TITRE : Utilisation des équipements et des ressources informatiques
--

6. CONFIDENTIALITÉ ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

6.1 Renseignements protégés

L'information contenue dans les équipements et les ressources informatiques est confidentielle lorsqu'elle a le caractère d'un renseignement nominatif ou d'un renseignement que l'office protège en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, ou le caractère d'un renseignement relatif à la vie privée de la personne au sens du Code civil du Québec.

6.2 Obligations de l'employé

6.2.1 Respect de la confidentialité des messages

L'employé doit respecter, lorsqu'il y a lieu, la confidentialité des messages transportés sur le réseau Internet et s'abstenir de lire, d'accéder, de modifier ou de détruire tout message, texte, données ou logiciel sans l'autorisation de leur propriétaire.

6.2.2 Respect de la réglementation des réseaux externes

L'employé doit respecter la réglementation des réseaux externes auxquels il accède, de même que l'intégrité des systèmes informatiques ainsi accessibles.

6.2.3 Respect des mécanismes de protection

L'employé doit respecter les mécanismes de protection de fichiers, de banques de données ou d'informations, d'ordinateurs, de systèmes ou du réseau Internet et ne pas tenter de les percer.

6.2.4 Transmission de documents confidentiels

L'employé doit éviter de transmettre des documents ou des informations de nature particulièrement sensible et confidentielle par courrier électronique, à moins de s'être assuré que des mesures de protection adéquates ont été prises.

7. SANCTIONS

7.1 Sanctions disciplinaires

L'employé qui contrevient aux dispositions de cette politique peut être l'objet, en plus des pénalités ou sanctions prévues par les lois et les règlements pertinents, des sanctions administratives suivantes :

- avis écrit;
- suspension d'un jour;
- suspension de cinq (5) jours;
- congédiement.

Le tout suivant les circonstances et la gravité de la situation.

POLITIQUE ET PROCÉDURE

TITRE : Utilisation des équipements et des ressources informatiques
--

8. COLLABORATION

L'employé doit collaborer avec l'office afin de faciliter l'identification et la correction de problèmes ou d'anomalies pouvant se présenter sur le réseau Internet ou concernant les équipements et les ressources informatiques.

9. ENTRÉE EN VIGUEUR

Cette politique entre en vigueur le jour de son adoption par le conseil d'administration.