Pour information : Direction générale du cadre gouvernemental de gestion du personnel
Tél. : 528-6227

C.T. 198872 du 1er octobre 2002

DIRECTIVE SUR L'UTILISATION ÉTHIQUE DU COURRIEL, D'UN COLLECTICIEL ET DES SERVICES D'INTERNET PAR LE PERSONNEL DE LA FONCTION PUBLIQUE

(Loi sur l'administration publique, L.R.Q., c. A-6.01, art. 31)

SECTION I. OBJET

1. Cette directive a pour but de préciser les attentes minimales auxquelles tout membre du personnel de la fonction publique doit répondre lors de l'utilisation d'un accès gouvernemental au courriel, à un collecticiel et aux services d'Internet, au moyen de l'équipement électronique gouvernemental mis à sa disposition, ou au moyen de l'équipement électronique de l'employé.

SECTION II. CHAMP D'APPLICATION

2. Cette directive s'applique à tout ministère ou organisme dont le personnel est nommé suivant la Loi sur la fonction publique (L.R.Q., c. F-3.1).

SECTION III. DÉFINITIONS

3. Dans cette directive, on entend par :

1° **« chiffrement »** : opération par laquelle est substitué à un texte en clair, un texte inintelligible et inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale;

2° **« collecticiel »** : logiciel qui permet à des utilisateurs reliés par un réseau de travailler en collaboration sur un même projet;

3° **« courriel »** : service de correspondance sous forme d'échange de messages électroniques, à travers un réseau informatique. Par extension, message transmis par un utilisateur vers un ou plusieurs destinataires, d'ordinateur à ordinateur, par l'intermédiaire d'un réseau informatique;

4° **« fichier »** : collection d'informations consignée et stockée comme une entité unique et spécifique sur un support de stockage;

5° **« Internet »** : réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole de communication TCP-IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs;

6° **« renseignement personnel »** : renseignement qui concerne une personne physique et qui permet de l'identifier ;

7° **« renseignement de nature confidentielle »** : renseignement dont la divulgation aurait des incidences néfastes, notamment sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs secrets industriels, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification;

8° **« réseau »** : système de transmission interconnectant tous les clients et les services ainsi que tout le matériel et les logiciels afférents.

SECTION IV. PRINCIPES

4. Le Conseil du trésor encourage l'utilisation des outils de travail électroniques par le personnel de la fonction publique, notamment parce qu'elle est susceptible d'améliorer la qualité des services aux citoyens, d'accroître la productivité et de faciliter la conciliation entre les obligations du travail et celles de la famille.

5. Les outils électroniques rendent possible l'identification de l'organisation de l'employé ou du gouvernement du Québec par un interlocuteur externe et il faut en tenir compte lors de leur utilisation.

6. Les attentes d'utilisation judicieuses des biens de l'État que la population a à l'égard de chaque membre du personnel de la fonction publique, peu importe son rang, ainsi que la responsabilité civile qui peut lier tout employeur, commandent de préciser le comportement attendu du personnel de la fonction publique à l'occasion de l'utilisation des moyens électroniques de travail.

SECTION V. RESPONSABILITÉS DU SOUS-MINISTRE OU DU DIRIGEANT D'ORGANISME

7. Le sous-ministre ou le dirigeant d'organisme prend les mesures nécessaires pour mettre en œuvre cette directive.

8. Le sous-ministre ou le dirigeant d'organisme peut adopter des lignes directrices internes qui reprennent les éléments et les obligations de la présente directive et les complètent en fonction des réalités de son organisation.

9. Le sous-ministre ou le dirigeant d'organisme doit s'assurer que cette directive ou les lignes directrices internes ont été communiquées à chaque membre de son personnel, et que des rappels périodiques sont effectués. Il doit aussi s'assurer, par engagement contractuel ou autrement, que cette directive ou les lignes directrices internes sont respectées par toute personne qui ne fait pas partie du personnel de l'organisation mais qui a accès à l'équipement électronique du ministère ou de l'organisme dont il a la charge ou au courriel, à un collecticiel, aux services d'Internet ou à un réseau réservé à l'usage du ministère ou de l'organisme.

SECTION VI. DISPOSITIONS GÉNÉRALES

10. Le sous-ministre ou le dirigeant d'organisme décide s'il est opportun d'accorder à un membre de son personnel le privilège d'utiliser un accès gouvernemental au courriel, à un collecticiel et aux services d'Internet.

    Le privilège est susceptible d'être révoqué en tout temps pour cause et ce, en conformité avec la présente directive ou des lignes directrices internes du ministère ou de l'organisme.

11. Le sous-ministre ou le dirigeant d'organisme s'assure qu'un employé qui utilise un accès gouvernemental au courriel, à un collecticiel ou aux services d'Internet, respecte, outre les obligations prévues dans la Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels (L.R.Q., c. A-2.1) :

    1° l'ensemble des règles et des pratiques en matière de sécurité de l'information et de protection des renseignements personnels;

    2° la législation en matière de droits d'auteurs;

    3° les règles d'utilisation de ces outils en vigueur au sein de l'organisation.

12. Un employé ne peut utiliser un accès gouvernemental au courriel, à un collecticiel et aux services d'Internet pour :

    1° harceler un autre membre du personnel de la fonction publique ou toute autre personne;

    2° visionner, télécharger, copier, partager ou expédier des images ou des fichiers érotiques, de pornographie juvénile ou de sexualité explicite ou dont le contenu a un caractère diffamatoire, offensant, harcelant, haineux, violent, menaçant, raciste, sexiste, ou qui contrevient à l'une des dispositions de la Charte des droits et libertés de la personne (L.R.Q., c. C-12), ainsi que de toute autre loi au Québec;

    3° télécharger tout logiciel ou partager ou copier un logiciel installé sur l'équipement gouvernemental auquel il a accès sans une autorisation préalable;

    4° utiliser à son profit les moyens électroniques mis à sa disposition;

    5° créer, expédier ou réexpédier tout message électronique ou fichier qui contient un élément qui contrevient aux paragraphes qui précèdent ou qui est susceptible d'affecter le fonctionnement de l'équipement mis à sa disposition ou d'un réseau gouvernemental auquel il est relié.

13. Le sous-ministre ou le dirigeant d'organisme peut exceptionnellement autoriser un membre de son personnel à utiliser un accès gouvernemental au courriel, à un collecticiel ou aux services d'Internet à des conditions différentes de celles énumérées à l'article 12 si la nature du travail effectué l'exige.

L'autorisation accordée par le sous-ministre ou le dirigeant d'organisme conformément au premier alinéa peut être révoquée en tout temps.

SECTION VII. PROTECTION DES RENSEIGNEMENTS PERSONNELS ET D'AUTRES RENSEIGNEMENTS DE NATURE CONFIDENTIELLE

14. Le sous-ministre ou le dirigeant d'organisme doit s'assurer qu'un membre de son personnel qui utilise un accès gouvernemental au courriel, à un collecticiel ou aux services d'Internet :

    1° respecte les dispositions de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels relatives à la collecte, à l'utilisation, à la communication, à la conservation ou, selon le cas, à l'archivage ou à la destruction d'un renseignement personnel;

    2° ne transmet aucun renseignement personnel ou tout autre renseignement de nature confidentielle qui n'a pas fait l'objet d'un chiffrement ou qui n'est pas protégé par tout autre dispositif de sécurité éprouvé.

SECTION VIII. CONTRÔLE

15. Toute information stockée ou consignée sur l'équipement électronique gouvernemental, au moyen du courriel, d'un collecticiel ou des services d'Internet ou par tout autre moyen est réputée constituer une information à laquelle le ministère ou l'organisme a accès.

16. Le sous-ministre ou le dirigeant d'organisme peut appliquer des mesures de gestion appropriées, selon les circonstances, à l'information qui est propre à un employé et que ce dernier a stockée sur l'équipement électronique gouvernemental.

17. Le sous-ministre ou le dirigeant d'organisme doit effectuer des vérifications régulières de l'utilisation d'un accès gouvernemental au courriel, à un collecticiel ou aux services d'Internet pour des motifs opérationnels et procéder à l'analyse de leurs résultats.

18. Le sous-ministre ou le dirigeant d'organisme peut décider de soumettre un membre de son personnel à une vérification particulière de l'utilisation d'un accès gouvernemental au courriel, à un collecticiel ou aux services d'Internet lorsqu'il existe des raisons de soupçonner que cette utilisation n'est pas conforme à cette directive, aux lignes directrices internes ou à la loi.

19. La mise en œuvre des mesures de gestion et des vérifications prévues dans cette section doit être faite conformément à la loi, notamment à l'égard de la protection de la vie privée, des renseignements personnels et des autres renseignements de nature confidentielle.

SECTION IX. SANCTIONS

20. Le sous-ministre ou le dirigeant d'organisme détermine, selon la nature ou la gravité du cas, s'il est opportun d'appliquer une sanction disciplinaire ou de prendre une mesure administrative lorsqu'un membre de son personnel contrevient à cette directive ou aux lignes directrices internes ou à la loi.

SECTION X. ENTRÉE EN VIGUEUR

Cette directive entre en vigueur le 1er octobre 2002.