



PAR COURRIEL

Le 2 février 2026

Objet : Demande d'accès aux documents – Accusé de réception et décision

N/Réf. : BSM-2026-005740

Bonjour,

Conformément à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, ci-après nommée « Loi sur l'accès »), nous avons traité votre demande d'accès reçue le 30 janvier 2026, laquelle se lit comme suit :

[...] En vertu de l'article 9 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, je désire obtenir copie de tout document ou fiche de breffage concernant l'utilisation des sites pornographiques par les employés de votre organisation, en particulier les hauts fonctionnaires, pour la période du 1^{er} janvier 2023 à aujourd'hui.

À des fins de recherche, je souhaite également connaître les dépenses annuelles totales en papiers-mouchoirs pour cette même période. [...].

(Transcription intégrale)

Décision

Nous donnons partiellement suite à votre demande. En effet, vous trouverez ci-joint la politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel ainsi que l'extrait pertinent du guide ministériel en éthique. Ces documents encadrent l'utilisation d'Internet par le personnel. Cependant, quant au second point de votre demande, le ministère de la Justice ne détient pas de document. La Loi sur l'accès ne porte que sur des documents détenus par un organisme public (article 1) et ce dernier

n'a pas l'obligation de produire un document nécessitant des calculs ou des comparaisons en vue de répondre à la demande d'accès (article 15).

Vous trouverez ci-joint copie des articles de loi sur lesquels se fonde notre décision.

Recours

Conformément à l'article 51 de la Loi sur l'accès, nous vous informons que vous pouvez, en vertu de la section III du chapitre IV de cette loi (articles 135 et suivants), faire une demande de révision à l'égard de cette décision en vous adressant à la Commission d'accès à l'information dans les 30 jours suivant la date de la présente décision. À cet effet, vous trouverez joint à la présente le document intitulé Avis de recours.

Nous vous prions d'agréer l'expression de nos sentiments les meilleurs.



Marie-Claude Daraiche, avocate
Responsable de l'accès aux documents
et de la protection des renseignements personnels

p. j. 4

Chapitre A-2.1

**LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR
LA PROTECTION DES RENSEIGNEMENTS PERSONNELS**

CHAPITRE I

APPLICATION ET INTERPRÉTATION

1. La présente loi s'applique aux documents détenus par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public ou par un tiers.

Elle s'applique quelle que soit la forme de ces documents: écrite, graphique, sonore, visuelle, informatisée ou autre.

1982, c. 30, a. 1.

[...]

CHAPITRE II

ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS

SECTION I

DROIT D'ACCÈS

[...]

15. Le droit d'accès ne porte que sur les documents dont la communication ne requiert ni calcul, ni comparaison de renseignements.

1982, c. 30, a. 15.

[...].

AVIS DE RECOURS

RÉVISION DEVANT LA COMMISSION D'ACCÈS À L'INFORMATION

a) POUVOIR

L'article 135 de la Loi prévoit qu'une personne peut, lorsque sa demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels ou dans le cas où le délai prévu pour répondre est expiré, demander à la Commission d'accès à l'information de réviser cette décision.

La demande de révision doit être faite par écrit; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (article 137).

L'adresse de la Commission d'accès à l'information est la suivante :

QUÉBEC

525, boulevard René-Lévesque Est
Bureau 2.36
Québec (Québec) G1R 5S9
Tél. : 418 528-7741
Numéro sans frais : 1 888 528-7741
Télécopieur : 418 529-3102

MONTRÉAL

2045, rue Stanley
Bureau 900
Montréal (Québec) H3A 2V4
Tél. : 514 873-4196
Numéro sans frais : 1 888 528-7741
Télécopieur : 514 844-6170

b) MOTIFS

Les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un enregistrement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) DÉLAIS

Les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (article 135).

La Loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (article 135).

APPEL DEVANT LA COUR DU QUÉBEC

a) POUVOIR

L'article 147 de la Loi sur l'accès stipule qu'une personne directement intéressée peut interjeter appel sur toute question de droit ou de compétence, devant le juge de la Cour du Québec, de la décision finale de la Commission, y compris une ordonnance de la Commission rendue au terme d'une enquête, ou, sur permission d'un juge de cette Cour, d'une décision interlocutoire à laquelle la décision finale ne pourra remédier.

b) DÉLAIS ET FRAIS

L'article 149 de la Loi sur l'accès stipule que l'appel est formé par le dépôt auprès de la Cour du Québec d'un avis à cet effet précisant les questions de droit ou de compétence qui devraient être examinées en appel.

L'avis d'appel doit être déposé au greffe de la Cour du Québec dans les 30 jours qui suivent la date de la réception de la décision finale par les parties.

c) PROCÉDURE

Selon l'article 151 de la Loi sur l'accès, l'avis d'appel doit être signifié aux parties et à la Commission dans les 10 jours de son dépôt au greffe de la Cour du Québec.

Le secrétaire de la Commission transmet au greffe, pour tenir lieu de dossier conjoint, un exemplaire de la décision contestée et les pièces de la contestation.



	Classification
Titre Politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel	Date d'entrée en vigueur 7 janvier 2019
Pour information Direction de la sécurité des actifs informationnels	Date dernière mise à jour 30 novembre 2018

DISPOSITIONS

1. Préambule

En assurant l'encadrement adéquat de l'utilisation des services des réseaux informatiques par les employés et les contractuels du ministère de la Justice du Québec (MJQ), celui-ci répond à la fois à son obligation de veiller sur la sécurité de l'information qu'il détient dans le cadre de sa mission conformément à la Directive sur la sécurité de l'information gouvernementale (Décret 7-2014 du 15 janvier 2014) et à celle de prendre les mesures nécessaires pour mettre en œuvre la Directive concernant l'utilisation éthique du courriel, du collecticiel et des services d'Internet par le personnel de la fonction publique (C.T. 198872 du 1^{er} octobre 2002). Cet encadrement lui permet également de se prémunir contre les risques technologiques, organisationnels et juridiques qui pourraient être engendrés par une utilisation abusive ou inappropriée de ces services.

2. Objet

La présente politique définit les lignes directrices en matière d'utilisation des services des réseaux informatiques par les personnes visées à l'article 4. Elle énonce également les rôles et responsabilités des principaux intervenants dans l'encadrement de cette utilisation et les sanctions prévues pour tout utilisateur qui contrevient aux dispositions énoncées.

Plus précisément, elle a pour objet de fixer les règles relatives à l'utilisation des services des réseaux informatiques du Ministère afin d'assurer, notamment, l'intégrité des systèmes et la protection des renseignements personnels et confidentiels. Elle vise aussi à sensibiliser l'utilisateur relativement à ses obligations quant à l'utilisation des services des réseaux informatiques mis à sa disposition dans le cadre de son emploi et les gestionnaires quant à leur responsabilité de veiller à la sécurité des actifs informationnels du Ministère.

Les services des réseaux informatiques comprennent le courriel, les services d'Internet et les collecticiels, y compris, sans s'y restreindre, la participation à des groupes de discussion, les médias sociaux, les services de partage ou toute autre application utilisant les services d'Internet, sans égard au type d'équipement ministériel utilisé.

3. Cadre légal et administratif

Les lois, règlements et autres textes normatifs sur lesquels s'appuie la présente politique sont énumérés à l'annexe I.

	Classification
Titre Politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel	Date d'entrée en vigueur 7 janvier 2019
Pour information Direction de la sécurité des actifs informationnels	Date dernière mise à jour 30 novembre 2018

4. Champ d'application

La présente politique s'adresse à tout utilisateur qui utilise les services des réseaux informatiques du Ministère, c'est-à-dire tout le personnel ainsi que toute autre personne dûment autorisée à y avoir accès, notamment un consultant, un partenaire, un fournisseur ou un employé d'un autre ministère ou organisme.

Elle ne s'applique pas aux juges des tribunaux visés à l'article 1 de la Loi sur les tribunaux judiciaires (RLRQ, c. T-16), aux juges de paix magistrats visés à l'article 161 de cette loi ainsi qu'aux juges du Tribunal des droits de la personne et du Tribunal des professions, ni au personnel affecté à la magistrature lorsque celui-ci exerce des fonctions de recherche, de secrétariat ou de support informatique auprès des juges.

La présente politique ne s'applique pas au personnel du Directeur des poursuites criminelles et pénales visé par la Loi sur le Directeur des poursuites criminelles et pénales (RLRQ c. D-9.1.1).

5. Lignes directrices

- 5.1. L'utilisateur peut faire usage des services des réseaux informatiques du Ministère à des fins professionnelles ainsi qu'à des fins personnelles limitées.
- 5.2. L'utilisation des services des réseaux informatiques à des fins personnelles constitue un privilège consenti par le Ministère. En conséquence, cette utilisation doit respecter les principes suivants :
 - a) se faire occasionnellement;
 - b) se limiter au strict minimum;
 - c) ne pas nuire aux activités professionnelles;
 - d) n'impliquer aucun frais supplémentaire et;
 - e) ne causer aucun préjudice au Ministère ainsi qu'à son image.
- 5.3. L'utilisateur ne peut utiliser un accès aux services des réseaux informatiques ministériel notamment pour :
 - a) télécharger tout logiciel incluant les gratuits, partager ou copier un logiciel installé sur l'équipement ministériel auquel l'utilisateur a accès, sans obtenir une autorisation préalable conformément à l'article 6.2 c);
 - b) créer sciemment une interférence sur le réseau local ou porter atteinte à la sécurité du réseau;
 - c) utiliser à son profit personnel ou professionnel lié à tout autre emploi rémunéré ou non, les équipements ministériels mis à sa disposition;
 - d) exprimer ses opinions, préférences politiques ou livrer des commentaires liées à l'activité judiciaire de manière incompatible avec ses obligations déontologiques ou son code d'éthique;
 - e) participer à une chaîne de lettre;
 - f) harceler ou importuner une personne;



	Classification
Titre Politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel	Date d'entrée en vigueur 7 janvier 2019
Pour information Direction de la sécurité des actifs informationnels	Date dernière mise à jour 30 novembre 2018

- g) visionner, télécharger, copier, partager, expédier ou conserver des images ou des fichiers érotiques, de sexualité explicite ou de pornographie juvénile ou dont le contenu a un caractère diffamatoire, offensant, harcelant, haineux, violent, menaçant, raciste, sexiste ou qui contrevient aux droits et libertés fondamentaux;
- h) créer, expédier ou réexpédier tout message électronique ou fichier qui contient un élément contraire aux prescriptions qui précèdent ou qui est susceptible d'affecter le fonctionnement de l'équipement mis à la disposition de l'utilisateur ou d'un réseau gouvernemental auquel il est relié;
- i) diffuser massivement des courriels de manière intentionnelle, à moins d'avoir obtenu l'autorisation préalable d'un gestionnaire;
- j) faire un usage qui irait à l'encontre des normes éthiques et déontologiques applicables.

5.4. La sous-ministre peut exceptionnellement autoriser un utilisateur, lorsque la nature des fonctions de ce dernier l'exige, à utiliser les services des réseaux informatiques à des conditions différentes de celles prévues à la présente politique.

5.5. L'utilisateur doit faire usage des services des réseaux informatiques à une fréquence et selon une durée qui est compatible avec sa prestation de travail.

5.6. La communication de renseignements personnels et confidentiels visés notamment par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1) et concernant une personne autre que l'usager lui-même, ne peut être effectuée par l'intermédiaire des services des réseaux informatiques à moins d'employer préalablement une méthode appropriée pour rendre cette information inintelligible ou inaccessible aux personnes autres qu'à celles à qui elle est destinée.

5.7. L'utilisation des services des réseaux informatiques doit se faire dans le respect des lois et règlements en vigueur au Québec, notamment la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, plus particulièrement quant à la collecte, l'utilisation, la communication, la conservation ou, selon le cas, l'archivage ou la destruction d'un renseignement personnel, la Loi concernant le cadre juridique des technologies de l'information (RLRQ c. C-1.1), la Loi sur les archives (RLRQ, c. A-21.1), la Loi sur la fonction publique (RLRQ, c. F-3.1.1) et la Loi sur le droit d'auteur (L.R.C. (1985), c. C-42).

5.8. Dans le cadre de ses fonctions, l'utilisateur des services des réseaux informatiques :

- a) emploie les codes d'accès, les mots de passe ou tout autre mécanisme de contrôle d'accès qu'il est autorisé à utiliser, sans les faire connaître aux personnes qui n'ont pas obtenu les mêmes accès y compris, sans s'y restreindre, au personnel d'assistance informatique ou ses gestionnaires;



	Classification
Titre Politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel	Date d'entrée en vigueur 7 janvier 2019
Pour information Direction de la sécurité des actifs informationnels	Date dernière mise à jour 30 novembre 2018

- b) utilise l'adresse courriel organisationnelle lors de l'inscription à des sites Internet, des forums de discussion ou des abonnements à des lettres de nouvelles, à moins d'une autorisation expresse de son gestionnaire;
- c) s'identifie dans tous ses messages électroniques;
- d) se soucie de préserver l'image du Ministère dans ses messages électroniques;
- e) veille à la conservation de ses courriels ou de ses échanges lorsqu'ils constituent des documents visés par le calendrier de conservation que l'on retrouve au Manuel de gestion documentaire du Ministère, approuvé en vertu de la Loi sur les archives;
- f) utilise un langage correct, poli et approprié et porte une attention particulière à la qualité de la langue française.

5.9. L'utilisateur qui s'inscrit sur des sites Internet, des forums de discussion ou des abonnements à des lettres de nouvelles dans le cadre d'une utilisation personnelle, fait usage de son adresse courriel personnelle.

5.10. L'utilisateur qui navigue sur les services des réseaux informatiques :

- a) effectue la cueillette d'information dans le respect des droits d'auteur;
- b) quitte immédiatement un site ou un forum dont le contenu contrevient aux dispositions de la présente politique ou peut nuire à l'image du Ministère;
- c) lorsqu'une authentification est requise, utilise un mot de passe dont la conception est logiquement différente de son mot de passe utilisé sur le réseau local du Ministère.

6. Rôles et responsabilités des principaux intervenants

6.1. Le Conseil de direction ministériel (CDM)

- a) Recommande l'approbation de la présente politique et la date de sa mise en vigueur auprès de la sous-ministre;
- b) Recommande la révision de la présente politique, si requis, suite à un changement du cadre légal et administratif qui la régit ou à un changement des orientations gouvernementales ou ministérielles;
- c) Désigne le ou les membres du CDM autorisés à approuver les demandes d'enquêtes administratives portant sur le respect de l'application de la présente politique à la suite de demandes formulées par un gestionnaire.

6.2. La Direction générale des technologies de l'information et des registres (DGTIR)

- a) Élabore et met en place des mécanismes de contrôle pour s'assurer du respect de la présente politique incluant un journal d'utilisation des services des réseaux informatiques du Ministère;



	Classification
Titre Politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel	Date d'entrée en vigueur 7 janvier 2019
Pour information Direction de la sécurité des actifs informationnels	Date dernière mise à jour 30 novembre 2018

- b) Surveille les réseaux informatiques afin d'en assurer la sécurité et identifie les événements de sécurité qui nécessitent une intervention particulière;
- c) Autorise, à des fins professionnelles, le téléchargement de logiciels, incluant les gratuits, ainsi que le partage ou la copie d'un logiciel installé sur l'équipement ministériel, dans le respect des règles relatives au droit d'auteur et aux exigences de sécurité du Ministère;
- d) Élabore un plan d'action pour correction des écarts suite à la réception des recommandations de la Direction de l'audit interne, des enquêtes et de l'évaluation de programmes (DAIEEP) et veille à sa mise en place;
- e) Révise la présente politique à la demande du CDM;
- f) Répond aux demandes de consultation des utilisateurs à l'égard des informations les concernant contenues au journal d'utilisation des services des réseaux informatiques du Ministère;
- g) Produit le journal d'utilisation des services des réseaux informatiques d'un utilisateur ciblé à la demande de la Direction des ressources humaines (DRH) et collabore aux enquêtes administratives de la DAIEEP, le cas échéant.

6.3. La Direction de l'audit interne, des enquêtes et de l'évaluation de programmes (DAIEEP)

- a) Procède, à l'égard d'un utilisateur ciblé, à une enquête administrative portant sur le respect de l'application de la présente politique à la suite d'une demande formulée par un gestionnaire et autorisée par un membre désigné du CDM.

6.4. La Direction des ressources humaines (DRH)

- a) S'assure du suivi de l'évolution des risques éthiques associés à l'utilisation des services des réseaux informatiques;
- b) Sensibilise le personnel à l'utilisation éthique des services des réseaux informatiques mis à leur disposition par le Ministère;
- c) En collaboration avec le gestionnaire, oriente la démarche à entreprendre vis-à-vis un employé soupçonné de ne pas respecter la présente politique;
- d) Procède à une enquête administrative portant sur la navigation Internet d'un utilisateur ciblé à la suite d'une demande formulée par un gestionnaire et autorisée par un membre désigné du CDM;
- e) Suite aux résultats de l'enquête administrative effectuée par la DAIEEP, la DRH détermine les mesures à prendre vis-à-vis l'employé et s'assure de la mise en application.

6.5. La Direction des communications (DCOM)

- a) Diffuse l'information pertinente relativement à l'application et au respect de la présente politique sur le site Intranet du Ministère dont le contenu a été élaboré en collaboration avec les directions concernées;



	Classification
Titre Politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel	Date d'entrée en vigueur 7 janvier 2019
Pour information Direction de la sécurité des actifs informationnels	Date dernière mise à jour 30 novembre 2018

- b) Diffuse, sur le site Internet du Ministère, un avertissement stipulant que les messages électroniques adressés aux personnes visées par la présente politique peuvent être contrôlés et surveillés par les autorités du Ministère;
- c) Coordonne l'application des normes concernant l'édition et la publication de documents sur les services des réseaux informatiques;
- d) Définit les orientations en matière d'utilisation des médias sociaux.

6.6. Le comité ministériel de la sécurité de l'information (CMSI)

- a) Détermine les éléments du journal d'utilisation des services des réseaux informatiques qui peuvent faire l'objet de surveillance constante;
- b) S'assure que les mécanismes en place répondent aux besoins de surveillance.

6.7. Le responsable organisationnel de la sécurité de l'information (ROSI)

- a) En collaboration avec les autres intervenants du Ministère, fait un bilan annuel au CMSI sur l'application de la présente politique et, s'il y a lieu, formule des recommandations ou propose des modifications à celle-ci au CDM.

6.8. Le conseiller organisationnel à la sécurité de l'information (COSI)

- a) Élabore un rapport de vérification de l'utilisation des réseaux informatiques du Ministère et le cas échéant, communique au ROSI les recommandations de redressement de situation;
- b) S'assure de la mise en place des contrôles de sécurité nécessaires pour assurer la confidentialité et l'intégrité du journal d'utilisation des réseaux informatiques du Ministère.

6.9. Le gestionnaire

- a) Veille à la participation de son personnel aux séances de sensibilisation ou d'information quant à l'utilisation des services des réseaux informatiques du Ministère;
- b) Veille, par la supervision de son personnel, à ce que les services des réseaux informatiques soient utilisés en conformité avec la présente politique;
- c) S'adresse à la DRH pour évaluer la pertinence d'une enquête administrative de la DAIEEP portant sur le respect de l'application de la présente politique. Le cas échéant, il adresse une demande d'autorisation d'enquête administrative auprès d'un membre désigné du CDM pour qu'il y ait une telle enquête à l'égard d'un utilisateur ciblé;
- d) S'assure, pour toute personne qui ne fait pas partie du personnel du Ministère et à laquelle il a permis l'accès aux services des réseaux informatiques, que la présente politique est respectée par l'entremise d'un engagement contractuel.



	Classification
Titre Politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel	Date d'entrée en vigueur 7 janvier 2019
Pour information Direction de la sécurité des actifs informationnels	Date dernière mise à jour 30 novembre 2018

6.10. L'utilisateur

- a) Prend connaissance de la présente politique et sur l'utilisation des services des réseaux informatiques et veille à s'y conformer;
- b) Prend des mesures raisonnables pour contrôler l'utilisation de son mot de passe ou tout autre mécanisme de contrôle d'accès qu'il est autorisé à utiliser en conformité avec les exigences de sécurité du Ministère;
- c) Participe aux séances de sensibilisation ou d'information quant à l'utilisation des services des réseaux informatiques du Ministère;
- d) Utilise les équipements et les services des réseaux informatiques de manière à éviter, dans la mesure du possible, l'encombrement que peuvent produire notamment les envois massifs, le téléchargement de fichiers volumineux ou l'écoute en continu;
- e) En regard de ses fonctions et le temps à y consacrer, évalue la pertinence avant d'adhérer à un forum de discussions et en avise son gestionnaire. Il informe ses interlocuteurs que son opinion n'engage que lui-même sauf s'il a pour mandat d'agir comme représentant du Ministère;
- f) Communique avec la DGTIR lorsqu'il désire consulter les informations le concernant contenues au journal d'utilisation des services des réseaux informatiques du Ministère;
- g) S'il possède un compte à privilèges élevés, s'assure de ne pas utiliser ce compte pour naviguer sur Internet.

7. Exigences en matière de surveillance

Toute information conservée ou transigeant sur l'équipement ministériel, au moyen des services des réseaux informatiques, est réputée constituer une information à laquelle le Ministère a accès. À cet égard, le Ministère possède les outils technologiques permettant de déchiffrer les communications initiées ou destinées à son réseau. Dans le but de ne pas intercepter indûment des données personnelles des utilisateurs, une liste des sites exclus du déchiffrement est maintenue et rendue accessible.

L'analyse des journaux d'utilisation des services des réseaux informatiques du Ministère est effectuée périodiquement afin de s'assurer du respect de la présente politique.

L'enquête administrative prévue à l'article 6.3 est effectuée lorsqu'il y a des motifs raisonnables de soupçonner qu'il y a une utilisation des services des réseaux informatiques qui n'est pas conforme à la présente politique. La lecture du contenu d'un courriel peut être effectuée uniquement dans le cadre d'une telle enquête et ne doit pas aller au-delà de ce qui est requis.

La mise en œuvre des mesures de contrôle prévues dans la présente section doit être faite conformément à la loi, notamment à l'égard de la protection de la vie privée, des renseignements personnels et confidentiels.

	Classification
Titre Politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel	Date d'entrée en vigueur 7 janvier 2019
Pour information Direction de la sécurité des actifs informationnels	Date dernière mise à jour 30 novembre 2018

8. Dispositions particulières

Le ROSI est chargé de la mise en application, du suivi et de la révision de la présente politique.

9. Sanction

Lorsqu'un utilisateur contrevient aux dispositions de la présente politique de même qu'aux dispositions énoncées au cadre légal et administratif de l'Annexe I, il s'expose à des mesures disciplinaires, administratives ou légales selon la faute commise. Ces mesures peuvent inclure la suspension des privilèges informatiques, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

ENTRÉE EN VIGUEUR ET APPROBATION

La présente politique entre en vigueur à compter 7 janvier 2019 et remplace celle en vigueur depuis le 23 avril 2003.

17/12/18

Date

François Gauthier

Signature

ANNEXE I – CADRE LÉGAL ET ADMINISTRATIF

CANADA

- Charte canadienne des droits et libertés de la Loi constitutionnelle de 1982;
- Code criminel, L.R., 1985, c. C-46;
- Loi sur le droit d'auteur, L.R., 1985, c. C-42.

QUÉBEC

Lois et règlements

- Code civil du Québec, RLRQ c. CCQ-1991;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1 :
 - Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, RLRQ, c. A-2.1, r. 2;
- Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1;
- Charte des droits et libertés de la personne, RLRQ, c. C-12;
- Loi sur la fonction publique, RLRQ, c. F-3.1.1 :
 - Règlement sur l'éthique et la discipline dans la fonction publique, RLRQ, c. F-3.1.1, r. 3;
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ, c. G-1.03;
- Loi sur le directeur des poursuites criminelles et pénales, RLRQ, c. D-9-1-1;
- Loi sur les archives, RLRQ, c. A-21.1

Directives et politiques

- Directive sur l'utilisation du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique, C.T. 198872 du 1^{er} octobre 2002;
- Directive sur la sécurité de l'information gouvernementale, Décret 7-2014 du 15 janvier 2014;
- Directive du ministère de la Justice sur la communication de renseignements confidentiels en vue d'assurer la protection des personnes;
- Politique ministérielle de sécurité de l'information;
- Politique ministérielle de gestion documentaire;
- Politique ministérielle sur l'éthique.

ANNEXE II – Définitions

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° « **message électronique** » : document informatisé qu'un utilisateur saisit, envoie ou consulte par l'intermédiaire d'un réseau. Comprend notamment le courriel, la messagerie instantanée, le forum de discussion, la publication sur un fil d'actualité, etc.

4° « **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.

5° « **fichier** » : collection d'informations consignée et stockée comme une entité unique et spécifique sur un support de stockage.

6° « **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.

7° « **renseignement personnel** » : renseignement qui concerne une personne physique et qui permet de l'identifier.

8° « **renseignement confidentiel** » : 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.

9° « **réseau** » : système de transmission interconnectant tous les clients et les services ainsi que tout le matériel et les logiciels afférents.

10° « **compte à privilèges élevés** » : compte réseau dont les droits octroyés permettent de gérer d'autres utilisateurs, d'installer des applications, d'administrer des serveurs ou des postes de travail, etc.

11° « **équipement ministériel** » : appareil permettant la mise en réseau d'information et dont l'acquisition et la configuration est réalisée par le Ministère. Comprend notamment les ordinateurs, les téléphones intelligents, les tablettes, etc.

GUIDE SUR L'ÉTHIQUE

UN OUTIL D'AIDE À LA RÉFLEXION



L'éthique,
une question
de jugement!

6 L'utilisation des biens et des ressources du Ministère



Loi sur la fonction publique	Règlement sur l'éthique et la discipline dans la fonction publique	Valeurs de l'administration publique et du Ministère
Article 5 et 9	Articles 7	Intégrité • Loyauté

Qu'est-ce qu'un bien et une ressource?

Les biens et les ressources du Ministère font référence à tout ce qui est mis à la disposition de l'employée ou de l'employé dans le cadre de son travail. Il peut s'agir des biens matériels, des ressources du Ministère ainsi que de ses commodités. Il peut s'agir également du travail accompli par ses collègues (notes, rapports, analyses, etc.).

Exemples de matériel, ressources et commodités utilisés par le personnel (sans s'y limiter) :

- Téléphone de bureau ou téléphone cellulaire;
- Tablette électronique;
- Photocopieur;
- Ordinateur portable ou de bureau;
- Services des réseaux informatiques (courriel, Internet, collecticiel);
- Applications;
- Bande passante (téléchargements, utilisation des données du Ministère);
- Tout document papier ou électronique;
- Etc.

Différentes utilisations possibles :

- Usage professionnel dans le cadre du travail au Ministère;
- Usage personnel pendant les heures de travail;
- Usage personnel en dehors des heures de travail.

Ce que dictent les règles en vigueur

Loi sur la fonction publique :

- Article 5 : Le fonctionnaire est tenu d'office d'être loyal et de porter allégeance à l'autorité constituée. Il doit exercer ses fonctions dans l'intérêt public, au mieux de sa compétence, avec honnêteté et impartialité et il est tenu de traiter le public avec égards et diligence;
- Article 9 : Le fonctionnaire ne peut, directement ou indirectement :
 - 1° accorder, solliciter ou accepter, en sa qualité de fonctionnaire, une faveur ou un avantage indu pour lui-même ou pour une autre personne;
 - 2° utiliser à son profit un bien de l'État ou une information qu'il obtient en sa qualité de fonctionnaire.

Règlement sur l'éthique et la discipline dans la fonction publique :

- Article 7 : Le fonctionnaire ne peut confondre les biens de l'État avec les siens. Il ne peut non plus utiliser au profit d'un tiers les biens de l'État ou une information dont il a pris connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions.

Il est aussi important de prendre connaissance des documents suivants :

- Directive sur l'attribution, l'utilisation et la gestion des appareils mobiles;
- Politique ministérielle de sécurité de l'information;
- Politique ministérielle sur l'utilisation du courriel, des services d'Internet et du collecticiel.

Utilisation personnelle des biens et ressources

Les fonctionnaires ne doivent pas confondre les biens de l'État avec les leurs ou les utiliser à leur profit¹⁹. Toutefois, au Ministère, un privilège est accordé au personnel. En effet, l'utilisation raisonnable à des fins personnelles des biens et des ressources est permise. Plus précisément, l'utilisation personnelle, pendant et en dehors des heures de travail, doit suivre les principes suivants²⁰:

- Être occasionnelle;
- Se limiter au strict minimum;
- Ne pas nuire aux activités professionnelles;
- N'impliquer aucuns frais supplémentaires;
- Ne causer aucun préjudice au Ministère;
- Ne pas nuire à la qualité du réseau Internet.

¹⁹ Décision de la Commission des lésions professionnel (CLP) : Lafontaine et Ministère des Transports, 2020 QCCFP : l'utilisation des caméras de surveillance du lieu de travail pour suivre un citoyen pose problème.

²⁰ Ces principes sont tirés de la *Politique ministérielle sur l'utilisation du courriel, des services d'Internet et du collecticiel*.

À noter

Le personnel doit préserver la **confidentialité de l'information** reçue dans l'exercice de ses fonctions, n'y accéder que si cela est nécessaire à l'exercice de ses fonctions et ne pas la communiquer à des personnes non autorisées. Il faut également éviter de divulguer de l'information qui pourrait nuire à l'intérêt public, à la réputation du Ministère ou du gouvernement, à son bon fonctionnement ou à la vie privée des citoyennes et citoyens. Vous ne pouvez contourner les mécanismes de sécurité mis en place ou agir de façon à nuire au bon fonctionnement de l'équipement ou de l'infrastructure technologique. Par exemple, il n'est pas permis de télécharger, partager ou copier un logiciel à des fins personnelles.

L'utilisation d'Internet ou du courriel ne peut, en aucun temps et sans s'y restreindre, servir à visionner, télécharger, copier, partager ou expédier des images ou des fichiers d'érotisme, de pornographie juvénile ou de sexualité explicite ou dont le contenu a un caractère diffamatoire, offensant, harcelant, violent, menaçant, raciste, sexiste.

Un tel comportement nuit gravement à la crédibilité et à la réputation du Ministère et ne peut pas être toléré. Notez que dans certains cas, des vérifications peuvent être effectuées quant à l'utilisation des biens du Ministère.

Remarque concernant l'habilitation sécuritaire : Veuillez noter que certains emplois au Ministère nécessitent une vérification des antécédents judiciaires. Pour obtenir davantage d'informations sur l'habilitation sécuritaire, le consentement à fournir et le processus suivi, vous pouvez consulter l'[aide-mémoire](#) sur les habilitations sécuritaires.

Spécification pour les appareils mobiles (autres que les ordinateurs portables)

L'utilisation personnelle des appareils mobiles du Ministère en dehors des heures de travail est permise si elle n'entraîne aucuns frais supplémentaires. Il faut retenir que l'appareil mobile appartient au Ministère²¹.

L'appareil mobile peut être :

- un téléphone (intelligent ou non);
- une tablette électronique;
- un téléavertisseur.

Spécification pour les voyages

La connexion hors Canada n'est pas permise avec les appareils informatiques du Ministère en raison des frais engendrés. Lors d'un voyage dans le cadre de votre travail, contactez votre gestionnaire pour connaître la marche à suivre.

Mises en situation

- 1 Le Ministère vous fournit, pour votre travail, un téléphone cellulaire. Pour une question d'efficacité, vous ne possédez que ce cellulaire. Vous l'utilisez donc à des fins personnelles. Vous partez prochainement pour des vacances à l'étranger et vous apporterez le cellulaire du Ministère. Pouvez-vous relever certains risques éthiques dans cette situation?

²¹ Voir la *Directive sur l'attribution, l'utilisation et la gestion des appareils mobiles*.

Questions de réflexion

- 1 Quels sont les éléments problématiques dans cette situation?
- 2 Quelles sont les parties concernées?
- 3 Quelles sont les conséquences pour chacune d'elles?
- 4 Est-ce qu'il y a des règles qui encadrent cette situation? Par exemple, est-ce possible d'utiliser le cellulaire à l'étranger?
- 5 Quelles valeurs interviennent dans cette situation?
- 6 Quelles sont les actions possibles?
- 7 Comment justifieriez-vous la décision de vos actions?

Piste de réflexion

Il existe plusieurs risques éthiques en lien avec l'utilisation personnelle du téléphone cellulaire prêté par le Ministère, et ce, tant pour le Ministère que la clientèle, les collègues et vous-même. Par exemple, en perdant le cellulaire, l'information confidentielle du Ministère ou celle des citoyennes et citoyens peut être compromise. Cela pourrait affecter la réputation et l'image du Ministère ou porter atteinte à la vie privée des citoyennes et citoyens. Votre intégrité et votre loyauté pourraient aussi être remises en question. Comment minimiser les risques?

D'abord, il faut se rappeler que l'utilisation du cellulaire à des fins personnelles est permise si elle n'occasionne pas de frais supplémentaires. Des frais supplémentaires peuvent être facturés si l'utilisation ne respecte pas le forfait cellulaire. De plus, il est interdit d'utiliser le cellulaire du Ministère à l'extérieur du Canada en raison des frais d'itinérance.

Ensuite, afin d'assurer la protection des informations confidentielles qui se trouvent dans le cellulaire (numéros de téléphone, courriels, documents, etc.), il est nécessaire de laisser en place les configurations de sécurité comme le mot de passe. De cette manière, elles seront protégées et les risques de fuite seront limités.

Enfin, l'utilisation du cellulaire du Ministère à des fins personnelles est un privilège. Par conséquent, non seulement faut-il être loyal lors de son utilisation, mais également discret. En d'autres mots, en tant que représentante ou représentant de l'administration publique, votre discrétion est importante surtout si le cellulaire est identifié explicitement comme étant un cellulaire du Ministère, et ce, pour ne pas nuire à la réputation ou à l'image du Ministère et de la fonction publique.

En cas de doute sur les utilisations permises, n'hésitez pas à contacter votre gestionnaire ou les personnes offrant un service-conseil en éthique. Il est recommandé également de consulter la Directive sur l'attribution, l'utilisation et la gestion des appareils mobiles.

Mises en situation

- 2 Vous êtes en télétravail et utilisez un ordinateur portable du Ministère pour votre emploi. Vous êtes de celles et ceux pour qui écouter de la musique augmente la productivité. Vous écoutez donc de la musique sur YouTube avec l'ordinateur du Ministère pendant votre travail. De plus, lors de vos pauses et de votre heure de dîner, vous faites un usage privé de l'ordinateur : vous envoyez des courriels avec votre adresse professionnelle, vous magasinez votre prochain voyage et vous faites des réservations pour vos sorties de la fin de semaine. Finalement, le soir venu, vous utilisez l'ordinateur portable pour écouter un film en famille sur une plateforme de visionnement en ligne (par exemple Netflix).

Questions de réflexion

- 1 Quels sont les éléments problématiques dans cette situation?
- 2 Quelles sont les parties concernées?
- 3 Quelles sont les conséquences pour chacune d'elles?
- 4 Est-ce qu'il y a des règles qui encadrent cette situation?
- 5 Quelles valeurs interviennent dans cette situation?
- 6 Quelles sont les actions possibles?
- 7 Comment justifieriez-vous la décision de vos actions?

Piste de réflexion

Cette situation comporte de nombreux enjeux éthiques et ces utilisations pourraient nuire au Ministère ou laisser croire que vous n'êtes pas intègre. Voici pourquoi.

Premièrement, l'accès à YouTube en même temps que l'utilisation du VPN peut occasionner des frais supplémentaires, car il s'agit de téléchargements qui utilisent la bande passante. De plus, les téléchargements de ce type peuvent ralentir le réseau informatique et nuire à sa qualité. Dans un tel cas, il s'agirait d'une utilisation déraisonnable selon les principes mentionnés. Il serait alors plus approprié d'utiliser votre propre téléphone cellulaire ainsi que votre réseau informatique personnel si vous tenez à écouter de la musique.

Quant à l'utilisation des outils de travail lors des pauses et de l'heure de dîner à des fins personnelles, il faut s'interroger sur la récurrence et sur la nature des sites consultés. D'abord, parce que l'utilisation personnelle doit être occasionnelle et se limiter au strict minimum. De plus, parce que certains sites contiennent parfois des publicités indésirables et déplacées qui peuvent laisser croire que vous visitez des sites interdits, même si ce n'était pas votre intention. C'est parfois le cas par exemple avec les sites de voyages.

L'utilisation du courriel professionnel doit être réservée uniquement au travail. De plus, il faut savoir qu'il est recommandé de limiter l'utilisation de votre boîte courriel personnelle sur le portable du Ministère, car tout ce qui est consulté ou téléchargé y laisse une trace.

Finalement, l'ordinateur étant un bien matériel prêté pour la prestation de travail, il ne devrait pas être utilisé pour le visionnement d'un film, même en dehors des heures de travail, notamment parce qu'il contient des informations confidentielles qui risquent d'être consultées par les autres membres de la famille.

Ces différents enjeux éthiques demandent d'utiliser votre jugement pour évaluer les risques associés à l'utilisation de l'ordinateur. Le mieux est certainement de garder une séparation claire entre l'utilisation professionnelle et l'utilisation personnelle des biens du Ministère, c'est-à-dire d'utiliser le moins possible les biens et ressources pour des usages personnels.

En bref : De façon générale, tout ce qui vous est rendu accessible dans le cadre de votre emploi ne devrait servir qu'à accomplir votre travail et être utilisé uniquement par vous. Retenez que l'utilisation personnelle de tout ce qui vous est accessible dans le cadre de votre emploi au Ministère (biens et ressources de l'État) doit être raisonnable et exercée dans les limites énoncées. Au mieux, faites une séparation claire entre vos activités professionnelles et personnelles en utilisant des appareils différents pour vos diverses utilisations.
