

De : [Julie Boucher](#)
À : [REDACTED]
Cc : [Boîte accès, mce](#)
Objet : N/Réf. : 2526-133 - Votre demande d'accès à l'information
Date : 19 février 2026 16:48:28
Pièces jointes : [133-document.pdf](#)
[AVIS DE RECOURS.pdf](#)

[REDACTED]

Objet : Votre demande en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1)

N/Réf. : 2526-133

Madame,

Nous donnons suite à votre demande d'accès du 30 janvier 2026, dont le but est d'obtenir copie de tout document ou toute fiche de breffage concernant l'utilisation des sites pornographiques par les employés du ministère du Conseil exécutif, en particulier les hauts fonctionnaires, ainsi que les dépenses annuelles totales en papiers-mouchoirs pour la période du 1^{er} janvier 2023 au 30 janvier 2026.

Vous trouverez jointe la Directive sur l'utilisation des services informatiques applicable à l'ensemble du personnel du ministère, incluant ses hauts fonctionnaires.

Nous vous informons que les recherches effectuées au ministère n'ont pas permis de retracer de documents présentant les dépenses annuelles en papier mouchoir.

Vous trouverez ci-joint copie de l'avis relatif au recours prévu à la section III du chapitre IV de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

Veuillez agréer, Madame, l'expression de nos sentiments les meilleurs.

Julie Boucher

Responsable de l'accès à l'information

Ministère du Conseil exécutif

835, boulevard René-Lévesque Est, 2^e étage

Québec (Québec) G1A 1B4

Téléphone : 418 643-7355

mce.accesmce@mce.gouv.qc.ca

Directive sur l'utilisation des services informatiques

1. Objet

Le ministère du Conseil exécutif (MCE) s'est doté d'une politique d'utilisation des services informatiques. Celle-ci fixe le cadre général d'une utilisation judicieuse et optimale des services informatiques, établit les rôles et responsabilités de chacun et fixe le cadre d'utilisation des services informatiques à des fins personnelles.

La présente directive sur l'utilisation des services informatiques vient préciser de quelle manière on doit faire usage des services mis à sa disposition par le Ministère. Elle fait donc état de positions claires en matière de bonnes pratiques et de comportement du personnel au cours de l'utilisation de l'équipement gouvernemental mis à sa disposition.

Dans un contexte d'utilisation de services informatiques aux multiples possibilités, notamment dans le cas du réseau Internet, la présente directive vient préciser les comportements et les limites en regard :

- de l'éthique;
- de la protection des renseignements personnels et de la confidentialité;
- de la sécurité;
- des choix du Ministère en ce qui concerne l'utilisation optimale des ressources.

Le mode d'application de la directive et les mesures de gestion quant à l'utilisation des services informatiques y sont également décrits.

2. Champ d'application

La présente directive s'applique à tout le personnel du Ministère nommé selon la *Loi sur la fonction publique (L.R.Q., c. F-3.1)*, de même qu'à toute personne agissant au nom du Ministère.

3. Définitions

- « 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.
- « Collecticiel » : logiciel qui permet à des utilisateurs reliés par réseau de travailler en collaboration à un même projet.
- « 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.

- « Cyberflânage » : utilisation d'Internet à des fins personnelles sur une base régulière.
- « Fichier » : collection d'informations consignées et stockées en tant qu'entité unique et spécifique sur un support de stockage.
- « Internet » : réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, reliés par le protocole de communication TCP-IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs.
- « Renseignement personnel » : donnée qui concerne une personne physique et qui permet de l'identifier.
- « Renseignement de nature confidentielle » : donnée dont la divulgation aurait des conséquences 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.
- « Réseau » : système de transmission interconnectant tous les clients et les services ainsi que tout le matériel et les logiciels afférents.
- « Réseaux sociaux » : ensemble des applications, des plateformes, des services et des outils qui permettent aux utilisateurs de partager de l'information et du contenu, et d'interagir entre eux.
- « Webtélé » : diffusion par Internet qui permet aux internautes de regarder du contenu vidéo.

4. Règles d'utilisation

4.1 En matière d'éthique

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), un employé qui utilise les services informatiques ministériels doit respecter :

- la Loi sur la fonction publique (L.R.Q., c. F-3.1.1), concernant notamment les normes d'éthique et de discipline;
- le Règlement sur l'éthique et la discipline dans la fonction publique (L.R.Q., c. F-3.1.1 r. 3, notamment sur les devoirs du fonctionnaire;
- la Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique (L.R.Q., c. A-6.01, art.31);
- les règles d'utilisation édictées dans la Politique de la sécurité de l'information;
- la loi en matière de droits d'auteur;
- les règles d'utilisation des outils en vigueur au Ministère, décrites dans la présente directive, dans la Politique de l'utilisation des services informatiques, dans les guides de bonnes pratiques mises à la disposition du personnel ou dans toute autre source d'information appropriée.

L'employé doit, en outre, utiliser les services informatiques mis à sa disposition de manière à préserver et à protéger, en tout temps, l'image du Ministère et du gouvernement du Québec.

Un employé ne peut utiliser les services informatiques mis à sa disposition pour :

- harceler un autre membre du personnel de la fonction publique ou toute autre personne;
- 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 tout autres lois du Québec;
- télécharger tout logiciel ou partager ou copier un logiciel, installé sur l'équipement gouvernemental auquel il a accès, sans autorisation préalable;
- créer, expédier ou réexpédier tout message électronique ou fichier contenant un élément contraire aux paragraphes qui précèdent ou susceptible d'affecter le fonctionnement de l'équipement ou d'un réseau gouvernemental auquel il est relié;
- s'adonner au cyberflânage.

Un employé ne peut, en outre, utiliser à son profit les moyens électroniques mis à sa disposition ou les utiliser de manière abusive à des fins personnelles, à l'extérieur du cadre établi à cette fin par la Politique de l'utilisation des services informatiques.

Les outils électroniques rendent possible l'identification du Ministère ou du gouvernement du Québec par un interlocuteur externe et on devra en tenir compte en cours d'utilisation.

De plus, l'employé qui utilise les réseaux sociaux devra en tout temps :

- s'abstenir de divulguer des données confidentielles ou stratégiques du MCE;
- s'assurer que ses activités en ligne n'entrent pas en conflit avec son emploi;
- communiquer à titre personnel en s'abstenant de faire mention du MCE ou du gouvernement du Québec.

4.2 En matière de protection des renseignements personnels et de confidentialité

Un employé qui utilise les services informatiques ministériels doit s'assurer de :

- respecter 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 et à la destruction d'un renseignement personnel;
- se conformer aux règles édictées dans la Politique de la sécurité de l'information;
- ne transmettre aucun renseignement personnel ni tout autre renseignement de nature confidentielle qui n'aient pas fait l'objet d'un chiffrement ou qui ne soient pas protégés par tout autre dispositif de sécurité éprouvé.

4.3 En matière de sécurité

Un employé qui utilise les services informatiques ministériels doit s'assurer de :

- protéger l'accès à son poste de travail par un mot de passe, lorsqu'il s'absente;
- préserver la confidentialité du ou des mots de passe qui lui sont attribués;
- ne pas modifier les paramètres des logiciels de sécurité installés sur son poste de travail, notamment le logiciel antivirus;
- détruire, sans même y avoir accédé, les documents et fichiers dont la provenance est douteuse;
- ranger sous clé tout équipement ou logiciel qui le nécessite;
- conserver les fichiers conformément au calendrier de conservation en vigueur au Ministère.

Un employé qui utilise les services informatiques ministériels ne doit pas :

- tenter d'avoir accès aux systèmes ou aux données à l'égard desquels il ne possède pas d'autorisation spécifique;
- installer un outil, logiciel ou autre élément présentant un risque pour la sécurité, notamment les logiciels de partage de fichiers poste à poste (P2P).

4.4 En matière d'utilisation optimale des ressources

Un employé qui utilise les services informatiques ministériels doit s'assurer de :

- restreindre l'utilisation personnelle d'Internet de façon à ne pas interférer avec sa prestation de travail ou celle de ses collègues et sous réserve des règles édictées dans la présente directive;
- ne pas utiliser à des fins personnelles la bande passante d'Internet de façon continue (par exemple, écoute de la radio sur Internet ou de webtélé);
- réduire la taille des fichiers volumineux par l'utilisation d'un utilitaire de compression approprié avant de transférer ces fichiers au moyen du courriel ou par un autre moyen;
- déposer, de manière structurée, les fichiers dans les répertoires mis à sa disposition sur l'infrastructure ministérielle (répertoires réseau);
- limiter le stockage, sur l'équipement électronique gouvernemental, de l'information qui lui est propre ou personnelle.

5. Mode d'application de la directive

Toute information stockée ou consignée sur l'équipement électronique gouvernemental est réputée constituer une information à laquelle le Ministère a accès. Des vérifications régulières de l'utilisation des services informatiques sont effectuées pour des motifs opérationnels, et les résultats de ces vérifications sont analysés.

À cette fin, le MCE s'est doté de mécanismes de contrôle de la sécurité sur ses réseaux pour :

- évaluer le rendement de ses composantes;
- cerner les problèmes et les régler;
- analyser les vulnérabilités;
- s'assurer du respect et de l'application de la présente directive.

Les données recueillies dans les registres d'accès peuvent, sans s'y limiter, être de la nature suivante :

- les services utilisés;
- le temps d'utilisation;
- les sites visités.

La mise en œuvre des mesures de gestion et des vérifications prévues dans la présente directive est 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.

Les moyens de contrôle, les guides de bonnes pratiques et autres éléments de mise en œuvre sont instaurés et transmis par l'intermédiaire des outils de communication ministériels, notamment l'intranet. Ils sont préalablement soumis à la consultation, lorsque celle-ci s'avère opportune.

Avis de recours

À la suite d'une décision rendue en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

Révision par la Commission d'accès à l'information

a) Pouvoir :

L'article 135 de la Loi prévoit qu'une personne dont la 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 peut 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 (art. 137).

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

Québec	525, boul. René-Levesque Est Bureau 2.36 Québec (Québec) G1R 5S9	Tél. : 418 528-7741 Numéro sans frais 1 888 -528-7741	Télec. : 418 529-3102
Montréal	500, boul. René Lévesque Ouest Bureau 18.200 Montréal (Québec) H2Z 1W7	Tél. : 514 873-4196 Numéro sans frais 1 888 -528-7741	Télec. : 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 renseignement, 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 (art. 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 (art. 135).