| RH-01 : Surveillance électronique des membres du personnel | EN VIGUEUR : 2023-01-23<br>RÉVISÉE LE : 2025-03-06 |
|---|---|

## OBJET

La présente directive administrative est présentée conformément à la métadirective ADM-01 : *Élaboration, révision et adoption d'une directive administrative* et découle de la limite opérationnelle de la direction de l'éducation 3.4 portant sur le traitement du personnel et des bénévoles et, à ce titre, fait l'objet d'un rapport annuel de monitoring.

De plus, la mise en œuvre de la présente directive est conforme aux modalités de la *Loi sur l'accès à l'information municipale et la protection de la vie privée de l'Ontario*.

Le Conseil scolaire catholique des Grandes Rivières (« le Conseil ») utilise la technologie afin de surveiller le lieu de travail, d'évaluer la productivité, de promouvoir le respect des directives du Conseil, des lois et règlements applicables et d'assurer la sécurité de son personnel, entre autres. La présente directive administrative décrit dans quelles circonstances et de quelles façons le Conseil surveille électroniquement le personnel, ainsi que les raisons pour lesquelles le Conseil peut utiliser l'information obtenue par la surveillance électronique.

## DESTINATAIRES

La présente directive administrative s'adresse aux membres du personnel du CSCDGR.

## DÉFINITIONS

« **Médias du Conseil** » veut dire tous les biens et ressources, peu importe leur emplacement, qui peuvent être utilisés pour enregistrer, traiter, ou transmettre les données électroniques du Conseil, quelles que soit la forme qu'elles prennent, y compris des réseaux, des bases de données, des serveurs, du matériel, des téléphones, des appareils mobiles, des dispositifs à mémoire électronique, des logiciels et des applications.

« **Surveillance électronique** » dénote l'emploi de moyens technologiques afin de surveiller, d'enregistrer et de recueillir des informations sur les activités des membres du personnel sur les lieux de travail.

## MODALITÉS D'APPLICATION

La présente directive administrative doit être appliquée en respect avec la politique administration 9112 – Accès à l'information et protection de la vie privée (en révision).

Toutes les informations qui sont créées, enregistrées, traitées, ou transmises à travers les médias du Conseil sont la propriété du Conseil, lequel se réserve le droit d'y accéder, de les utiliser, et de les surveiller. En conséquence, les membres du personnel ne peuvent avoir aucune attente raisonnable de protection de leur vie privée en milieu de travail. Aux fins de protéger sa vie privée, le membre du personnel doit être conscient du fait que la surveillance électronique risque de révéler des renseignements personnels confidentiels à son sujet et agir en conséquence. Ces renseignements peuvent comprendre des communications que le membre du personnel envoie ou reçoit, ainsi que des informations que le membre du personnel crée, des informations auxquelles le membre du personnel accède, ou des informations que le membre du personnel enregistre ou entrepose sur les médias du Conseil.

### COMMUNICATION

Le Service des ressources humaines et de la paie et le Service de l'informatique sont responsables de l'administration de la présente directive.

Le Conseil fournira à tous les membres du personnel une copie de la présente directive administrative dans les 30 jours suivant la date à laquelle elle a été mise en vigueur. Le Conseil fournira une copie de la directive à chaque nouveau membre du personnel dans les 30 jours suivant son embauche. Le Conseil fournira également une copie de la présente directive à chaque travailleur temporaire qui fournit des services au Conseil par le biais d'une agence d'aide temporaire, et ce, dans les 24 heures suivant le début de la tâche dudit travailleur.

### AMENDEMENTS

Le Conseil peut, de temps en temps, modifier ou mettre à jour la présente directive administrative. Le cas échéant, le Conseil fournira aux membres du personnel une copie de la directive mise à jour, et ce, dans les 30 jours suivant la mise à jour ou conformément à tout délai prévu par une loi ou un règlement.

## PROCESSUS

### MÉTHODES ET BUTS DE SURVEILLANCE ÉLECTRONIQUE

Le tableau suivant fait état : (1) des méthodes par lesquelles le Conseil mène la surveillance électronique; (2) des circonstances dans lesquelles le Conseil mène la surveillance électronique, et; (3) des façons dont le Conseil peut utiliser les informations qu'il recueille par l'entremise de la surveillance électronique.

La plupart des activités de surveillance électronique sont de nature passive, c'est-à-dire qu'elles s'effectuent automatiquement par l'entremise de systèmes pare-feu ou d'enregistrement de données ou de communication. Malgré ce qui précède :

- la surveillance électronique peut avoir lieu à tout moment, sans préavis, pendant les heures de travail et à d'autres moments en lien avec les activités du travail, l'utilisation des ressources du Conseil, ou l'utilisation des médias du Conseil, et;
- tous les cas de surveillance électronique peuvent être utilisés :
    - dans le cadre d'instances juridiques impliquant le Conseil (y compris devant des arbitres ou des tribunaux);
    - dans le but d'assurer le respect des politiques et des directives administratives du CSCDGR de même que des lois pertinentes;
    - pour protéger l'infrastructure électronique du Conseil et ses ressources électroniques;
    - pour vérifier tout abus potentiel des ressources du Conseil (y compris le vol de temps);
    - afin d'assurer la continuité des opérations du Conseil (en outre, lors du départ ou de l'absence d'un membre du personnel);
    - pour prévenir ou répondre aux inconduites liés au travail, y compris à des fins de coaching ou de discipline;
    - pour assurer le bien-être, la santé et la sécurité des membres de la communauté scolaire, y compris les élèves et les personnes ayant accès aux établissements du Conseil.

| Méthode | Circonstances | But(s) |
|---|---|---|
| Surveillance des courriels et des communications | Utilisation des médias et des systèmes de communication du Conseil (ex : courriel, appels téléphoniques internes et externes, plateformes de messagerie) | • Évaluer et améliorer la performance et la productivité<br>• Intervenir et monitorer l'utilisation excessive ou inappropriée des médias du Conseil<br>• Prévenir et intervenir dans les incidents reliés au non-respect des politiques, des directives administratives ou des lois et règlements applicables |
| Logiciel de sécurité | Utilisation de logiciel de pare-feu et les systèmes de sécurité intelligent permettant de protéger l'infrastructure du Conseil (réseaux, serveurs, base de données).<br>Assure un contrôle et une gestion appropriée des accès lorsqu'un membre utilise les réseaux et les | • Assurer un monitorage passif des activités de communication et de vidéosurveillance<br>• Assurer un contrôle de vérification et d'identification des accès aux bases de données conformément aux lois et règlements applicables, les politiques et les directives administratives en vigueur |

| | | |
|---|---|---|
| | outils de communications électroniques du Conseil. | • Intervenir et prévenir des activités d'hameçonnage<br>• Prévenir et intervenir dans les incidents reliés au non-respect des politiques, des directives administratives ou des lois et règlements applicables |
| Surveillance des activités sur les réseaux | Utilisation des médias du Conseil (ex: les données et l'activité Internet) | • Évaluer et améliorer la performance et la productivité<br>• Intervenir et monitorer l'utilisation excessive ou inappropriée des médias du Conseil<br>• Prévenir et intervenir dans les incidents reliés au non-respect des politiques, des directives administratives ou des lois et règlements applicables |
| Surveillance d'appareils | Utilisation des ordinateurs, des appareils portables, et autres matériaux techno-logiques du Conseil | • Évaluer et améliorer la performance et la productivité<br>• Intervenir et monitorer l'utilisation excessive ou inappropriée des médias du Conseil<br>• Prévenir et intervenir dans les incidents reliés au non-respect des politiques, des directives administratives ou des lois et règlements applicables |
| Cartes-clés, jetons d'accès | Utilisation de points d'accès aux lieux du Conseil | • Surveiller la fréquentation et les heures travaillées<br>• Protéger la sécurité physique des membres du personnel, des invités, des lieux, et des membres du public |
| Surveillance vidéo | Activités sur les lieux physiques du Conseil | • Assurer le bien-être, la santé et la sécurité physique des membres du personnel, des invités, des lieux, et des membres de la communauté scolaire et du public, y compris les élèves |
| Surveillance des médias sociaux | Emploi de comptes de médias sociaux personnels ou ceux du Conseil | • Gérer les relations publiques<br>• Intervenir et monitorer l'utilisation excessive ou |

| | | |
|---|---|---|
| | | inappropriée des médias du Conseil<br>• Prévenir et intervenir dans les incidents reliés au non-respect des politiques, des directives administratives ou des lois et règlements applicables |
| Terminaux biométriques | Utilisation des points d'accès aux lieux du Conseil | • Limiter aux utilisateurs autorisés l'accès aux lieux du Conseil et aux appareils<br>• Surveiller l'assiduité des membres du personnel et enregistrer les heures de travail |

**RÉFÉRENCES ET FONDEMENTS LÉGISLATIFS**

- *Loi de 2000 sur les normes d'emploi*
- *Loi sur l'accès à l'information municipale et la protection de la vie privée*

**DIRECTIVES ADMINISTRATIVES ASSOCIÉES**

- Politique 9112 – Accès à l'information et la protection de la vie privée (en révision)
- Politique 6126 – Utilisation de caméras de vidéosurveillance (en révision)
- TIC-01 – Utilisation responsable des technologies de l'information et des communications

**ANNEXES**

- Sans objet.