

ADMINISTRATION - TECHNOLOGIE**UTILISATION RESPONSABLE DES TECHNOLOGIES
DE L'INFORMATION ET DES COMMUNICATIONS (TIC)**

Approuvée le 19 juin 2025
Prochaine révision en 2028-2029

Page 1 de 5

1. CONTEXTE

- 1.1. Le Conseil scolaire Viamonde reconnaît l'importance d'utiliser les technologies de l'information et des communications (TIC) pour soutenir les élèves dans leur apprentissage, faciliter le travail des membres du personnel et appuyer toutes autres personnes autorisées à utiliser les TIC au sein du Conseil. En plus de répondre aux besoins des parties prenantes, il est primordial de veiller à ce que les TIC soient utilisées de façon responsable en respectant les règles usuelles de bienséance et de courtoisie, ainsi que les valeurs du Conseil.

2. APPLICATION

- 2.1. Les technologies de l'information et des communications comprennent l'ensemble de l'équipement informatique et des ressources technologiques permettant de transmettre, d'enregistrer, de créer, de modifier, de partager ou d'échanger des informations, y compris, sans s'y limiter: les serveurs, les réseaux, les ordinateurs, les tablettes, les téléphones cellulaires, les accessoires périphériques de lecture, d'emmagasiner, de reproduction, d'impression, de transmission, de réception et de traitement de l'information, l'équipement de télécommunication ainsi que les logiciels et les applications web autorisés.
- 2.2. Les parties prenantes utilisant les TIC désignent les personnes autorisées à accéder aux TIC du Conseil par le biais de toute activité électronique ou de communication avec n'importe quel appareil (que ces appareils leurs appartiennent ou non, ou ait été fourni par le Conseil) et quel que soit l'emplacement physique des parties prenantes.
- 2.3. Les parties prenantes utilisant les TIC acceptent par leurs utilisations, les conditions prescrites dans cette politique et les directives administratives afférentes.

3. UTILISATION ACCEPTABLE

- 3.1. L'accès et l'utilisation des TIC sont autorisés à des fins pédagogiques, administratives et éducatives conformément à la mission et à la vision du Conseil.
- 3.2. L'utilisation responsable des TIC renforce l'efficacité au travail, le respect et bienveillance, est au service de l'apprentissage et de l'enseignement, et conforme au code des droits de la personne de l'Ontario (le Code).

4. GESTION SÉCURITAIRE DES DONNÉES ET CONFIDENTIALITÉ

- 4.1. Le Conseil est propriétaire de toutes les ressources informatiques et peut accéder aux données et informations que les parties prenantes créent, stockent, envoient ou reçoivent en utilisant les TIC du Conseil.

ADMINISTRATION - TECHNOLOGIE**UTILISATION RESPONSABLE DES TECHNOLOGIES
DE L'INFORMATION ET DES COMMUNICATIONS (TIC)****Page 2 de 5**

-
- 4.2. Les parties prenantes doivent être prudentes lorsqu'elles utilisent les ressources TIC du Conseil à des fins personnelles. L'utilisation personnelle des TIC du Conseil est un choix qui implique une renonciation à la protection de ses renseignements personnels et de sa vie privée. Les parties prenantes souhaitant s'assurer que leurs documents et communications de nature personnelle restent privées, ne doivent pas se connecter ou utiliser les ressources technologiques du Conseil pour ces fins.
 - 4.3. Les parties prenantes qui utilisent les TIC du Conseil sont responsables d'assurer de maintenir la confidentialité et la sécurité des données du Conseil auxquelles elles ont accès.
 - 4.4. Le Conseil met en place des pratiques pour attribuer, superviser et restreindre l'accès aux données et aux systèmes, en le limitant uniquement aux parties prenantes qui en ont besoin pour remplir leurs responsabilités liées à la mission et à la vision du Conseil.
 - 4.5. Le Conseil met en œuvre des pratiques pour contrôler et sécuriser les données confidentielles en sa possession afin de minimiser le risque d'atteinte à la vie privée ou le risque de perte de données confidentielles.
 - 4.6. Les parties prenantes doivent prendre toutes les précautions raisonnables pour éviter une violation de la vie privée en s'assurant que les données sont sécurisées et que celles-ci sont utilisées uniquement aux fins prévues et autorisées conformément à la politique et directive administrative 2,106 Accès à l'information et protection de la vie privée et aux directives administratives de cette politique.

5. SÉCURITÉ DES RÉSEAUX ET TECHNOLOGIES

- 5.1. La sécurité des réseaux et technologies relève de l'ensemble des parties prenantes utilisant les TIC. Les parties prenantes doivent intégrer au quotidien les meilleures pratiques pour réduire les risques liés à la cybersécurité.
- 5.2. Le Conseil met en place des pratiques et des technologies nécessaires pour veiller à ce que le réseau informatique demeure sécuritaire et performant. Les parties prenantes utilisant les TIC doivent respecter en tout temps, les dispositions de sécurité mises en place par le Conseil.
- 5.3. Le Conseil met à la disposition des parties prenantes des ressources et des formations à l'appui du développement des compétences en cybersécurité.
- 5.4. Le Conseil met en place un cadre de référence pour la gestion des cyberincidents.
- 5.5. Toute partie prenante qui contourne les contrôles de cybersécurité mis en œuvre par le Conseil peut voir son accès révoqué et faire face à des mesures disciplinaires.

6. ASSIGNATION D'ÉQUIPEMENT TIC

- 6.1. Le Conseil autorise que certains équipements TIC tels que les ordinateurs portatifs, les téléphones cellulaires et les périphériques informatiques puissent être assignés à des membres du Conseil, des membres du personnel, ou à des élèves pour des raisons pédagogiques ou administratives.

ADMINISTRATION - TECHNOLOGIE**UTILISATION RESPONSABLE DES TECHNOLOGIES
DE L'INFORMATION ET DES COMMUNICATIONS (TIC)****Page 3 de 5**

-
- 6.2. Chaque partie prenante qui reçoit un équipement TIC doit au préalable signer une entente de responsabilité et accepter toutes les conditions d'utilisation.
 - 6.3. Les parties prenantes sont responsables des équipements qui leur sont assignés et pourraient être tenues de rembourser le Conseil pour la perte de l'équipement ou tout dommage causé à l'équipement lorsque celui-ci est en leur possession.

7. UTILISATION DES APPAREILS PERSONNELS

- 7.1. Le Conseil permet aux élèves et aux membres du personnel d'utiliser leur appareil numérique personnel et de le brancher à Internet au moyen d'un de ses réseaux sans fil et ce, à des fins strictement pédagogiques ou administratives.
- 7.2. Le branchement des appareils numériques personnels à un réseau sans fil du Conseil constitue un privilège et non un droit. Le Conseil peut, à sa seule discrétion, refuser ou retirer l'accès à son réseau, et ce, à tout moment, ou interdire l'utilisation des appareils numériques personnels à des personnes se trouvant sur l'une de ses propriétés.
- 7.3. Le Conseil peut accorder, à sa discrétion, l'accès au réseau sans fil aux personnes qui visitent les lieux du Conseil.
- 7.4. Les parties prenantes accédant au réseau du Conseil avec leurs appareils numériques personnels doivent s'assurer que toutes les mises à jour de sécurité ont été installées sur leurs appareils et que ceux-ci sont exempts de tout logiciel malveillant.

8. COMMUNICATIONS ÉLECTRONIQUES ET UTILISATION DES MÉDIAS SOCIAUX

- 8.1. Les membres du Conseil et les membres du personnel doivent utiliser uniquement les moyens autorisés par le Conseil lors de communication électronique avec les membres du personnel, les élèves et la communauté scolaire.
- 8.2. Les médias sociaux constituent des outils valables et efficaces dans le contexte de l'apprentissage puisqu'ils peuvent permettre la promotion et la prestation des programmes éducatifs. Le Conseil permet l'utilisation des médias sociaux en lien avec un encadrement pédagogique spécifique, et ce, conformément aux règlements du ministère de l'Éducation.
- 8.3. Le Conseil peut limiter l'accès et encadrer l'utilisation des médias sociaux.
- 8.4. Le Conseil permet aux membres du personnel d'utiliser les médias sociaux dans l'exercice de leurs fonctions ainsi que pour promouvoir le Conseil, ses initiatives et ses programmes, en autant que les communications sont faites de manière éthique, bienveillantes, conforme aux valeurs du Conseil et au Code.
- 8.5. L'adresse de courriel assignée aux membres du Conseil, aux membres du personnel et aux élèves ne peut être utilisée que pour des fins pédagogiques ou professionnelles.

ADMINISTRATION - TECHNOLOGIE**UTILISATION RESPONSABLE DES TECHNOLOGIES
DE L'INFORMATION ET DES COMMUNICATIONS (TIC)****Page 4 de 5**

9. INTERDICTIONS

- 9.1. Le Conseil doit assurer la sécurité et le bien-être des élèves, des membres du personnel et des membres du Conseil et protéger sa réputation. Ainsi, le Conseil proscrit :
- l'usage abusif ou excessif des TIC, incluant l'envoi de courriels à des fins personnelles au moyen du système de messagerie du Conseil, que ceux-ci soient envoyés pendant ou après les heures de travail;
 - l'utilisation personnelle des TIC ayant un impact néfaste sur les opérations du Conseil ou qui diminue le temps consacré à son emploi;
 - le contournement des contrôles de cybersécurité en place;
 - la publication d'images en direct ou de mises à jour qui divulguent la localisation des élèves en sortie scolaire;
 - la publication de photos, vidéos et travaux d'élèves sans le consentement préalable par écrit de la personne détenant l'autorité parentale ou de l'élève ayant plus de 18 ans.
 - la consultation de certains sites, tels que les sites à connotation sexuelle ou de violence;
 - la consultation de sites diffusant du matériel à caractère diffamatoire, offensant, harcelant, haineux, violent, menaçant, raciste, sexiste, ou homophobe;
 - le harcèlement ou la cyberintimidation;
 - l'utilisation des TIC à des fins illégales, inappropriées, ou obscènes ou encore pour appuyer de telles activités;
 - l'utilisation des TIC à des fins commerciales sans l'approbation du Conseil;
 - l'installation de logiciels ou d'application non autorisés sur les appareils du Conseil; ou
 - l'usage des TIC à des fins non conformes au Code.

10. CONSÉQUENCES DE LA VIOLATION

- 10.1. Tout usage qui enfreint la présente politique, y compris les lois et les règlements fédéraux, provinciaux, ainsi que les autres politiques du Conseil, de l'école et de la salle de classe s'y rattachant, peut, selon la gravité de la situation, mener:
- à la suspension ou à la révocation du privilège d'accès aux TIC du Conseil et de l'école, avec ou sans préavis;
 - au remboursement au Conseil des frais pour les dommages causés ou les réparations nécessaires à la suite du non-respect des politiques et directives administratives en place;
 - dans le cas des élèves, à une imposition de sanctions prévues dans le Code de conduite du Conseil ou de l'école (p. ex., une suspension ou un renvoi);
 - dans le cas des membres du personnel, à des mesures disciplinaires selon les dispositions prévues dans la politique 5,206 - Mesures disciplinaires du Conseil;
 - à une poursuite judiciaire par les autorités compétentes; ou
 - à toute autre mesure administrative, disciplinaire ou légale jugée appropriée par le Conseil.

ADMINISTRATION - TECHNOLOGIE**UTILISATION RESPONSABLE DES TECHNOLOGIES
DE L'INFORMATION ET DES COMMUNICATIONS (TIC)****Page 5 de 5**

11.DIRECTIVES ADMINISTRATIVES CONNEXES

Directives administratives 2,400a – *Accès au réseau sans fils avec un appareil numérique personnel*

Directives administratives 2,400b – *Communications par moyen électronique*

RÉFÉRENCES

Politique 2,106 *Accès à l'information et protection de la vie privée et aux directives administratives*