| RECUEIL DE GESTION | | | POLITIQUE |
|---|---|---|---|
| Centre de services scolaire des Draveurs Québec | | SECTEUR | Service du secrétariat général et des communications |
| SUJET | POLITIQUE SUR LA CYBERCITOYENNETÉ ET LA CYBERSÉCURITÉ | | |
| IDENTIFICATION | CODE : 50-45-01 | | PAGE : 1 de 5 |

| RÉSOLUTION NO : | AMENDEMENT NO : | DATE | SIGNATURE |
|---|---|---|---|
| C217-2204 | | 2022-04-04 | Original signé par la Présidence du conseil d'administration |

## 01) RÉFÉRENCES

La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, Loi 133)

La Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1)

La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics

Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2)

Centre canadien pour la cybersécurité (https://cyber.gc.ca/fr/)

Pensez cybersécurité (pensezcybersecurite.gc.ca)

La politique 50-39-01 sur la sécurité de l'information

Conventions collectives en vigueur

## 02) PRÉAMBULE

La Politique sur la cybercitoyenneté et la cybersécurité constitue un ensemble intégré de principes et d'objectifs qui décrit, en matière de disponibilité, de confidentialité, de protection et d'éthique les comportements à adopter concernant la prestation de services et les actifs informationnels à l'ère du numérique. Ces prestations de service ainsi que les actifs informationnels peuvent être liés de près ou de loin à toutes les composantes organisationnelles du Centre de services scolaire des Draveurs (CSSD). En ce sens, les principes énoncés dans cette politique doivent être appliqués conjointement avec la Politique sur la sécurité de l'information et toutes autres procédures ou directives en découlant. Enfin, notons que cette politique permet au CSSD d'accomplir sa mission, de préserver sa réputation et celle des membres

de son personnel, de respecter les lois et de réduire les risques en protégeant l'actif informationnel qu'il a créé ou reçu.

## 03) CHAMP D'APPLICATION

La politique sur la cybercitoyenneté et la cybersécurité s'applique, selon le contexte, à tous les membres du personnel, élèves du CSSD et toute personne ou tout organisme qui constitue un tiers qui utilisent ou ont accès à un actif informationnel ou un média numérique relevant de la compétence du CSSD. Les modalités d'application de la politique peuvent s'étendre au-delà des heures de travail normées ou de l'horaire des classes et, dans certaines situations particulières, au-delà de la durée d'un contrat de travail.

## 04) DÉFINITIONS

Dans la présente politique, à moins d'indication contraire, les mots suivants signifient :

- **Actif informationnel** : une information, quels que soient son canal de communication (téléphone analogique ou numérique, télégraphe, télécopie, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.

- **Communication numérique** : toutes les communications qui se font au moyen d'un média numérique : Web, médias sociaux, applications mobiles, messageries instantanées, télévision connectée, bornes interactives, espaces publicitaires numériques, géolocalisation ainsi que tout autre objet connecté.

- **Confidentialité** : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

- **Cybermenace** : est une activité qui vise à compromettre la sécurité de l'environnement numérique de l'organisation en modifiant la disponibilité, l'intégrité ou la confidentialité des systèmes ou des actifs informationnels qu'ils contiennent.

- **Cybercitoyenneté** : se rapporte aux normes et aux valeurs du vivre-ensemble dans un environnement numérique.

- **Cybersécurité** : englobe tous les moyens qui permettent d'assurer la protection, la confidentialité et l'intégrité des données, sensibles ou non, au sein d'un environnement numérique.

- **Disponibilité** : Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

- **Environnement numérique** : espace structuré par des instruments technologiques divers, permettant aux usagers d'accéder à des actifs informationnels, de communiquer et de collaborer en

ligne.

- **Empreinte numérique** : traces ou « empreintes » que les gens laissent en ligne. Il s'agit d'informations transmises en ligne, telles que l'inscription à un forum, les courriers électroniques et les pièces jointes, le téléchargement de vidéos ou d'images numériques et toute autre forme de transmission d'informations concernant un individu.

- **Intégrité** : Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

- **Médias numériques :** Ensemble de médias faisant référence à des techniques de production et de communication de l'information qui, en intégrant le numérique et/ou l'interactivité, permettent la création, le traitement et la distribution de contenus multimédias.

- **Nétiquette :** est l'ensemble des conventions de bienséance régissant le comportement des internautes dans le réseau, notamment lors des échanges dans les forums ou par courrier électronique.

- **Utilisateur** : toute personne de l'organisation de quelque catégorie d'emploi, élève ainsi que toute personne qui, par engagement contractuel ou autrement, utilise un actif informationnel ou un média numérique de l'organisation ou y a accès, et ce, peu importe le lieu et l'heure du jour et de la nuit.

## 05) OBJECTIFS

**5.1** Sensibiliser la communauté éducative en ce qui concerne le civisme dans un environnement numérique.

**5.2** Favoriser et encourager l'adoption de comportements cybersécuritaires.

**5.3** Assurer la protection et la résilience des services publics et des échanges électroniques au sein du CSSD.

**5.4** Préserver la confiance des membres de la communauté, parents, élèves et membres du personnel à l'égard de la sécurité de leurs données.

## 06) PRINCIPES ET ENGAGEMENTS

**6.1** L'application de mesures de protection doit être proportionnelle à la valeur de l'information et aux risques encourus.

**6.2** Les principes de disponibilité, d'intégrité et de confidentialité par rapport aux actifs informationnels doivent être intégrés au sein de toutes les unités administratives.

**6.3** L'utilisation des actifs informationnels et des médias numériques relevant de la compétence du CSSD, peu importe l'environnement physique de travail et l'heure du jour ou de la nuit, doit être

faite en respectant des normes élevées en matière de cybercitoyenneté et de cybersécurité.

**6.4** Une vision globale, concertée et évolutive de l'utilisation des actifs informationnels et de la citoyenneté dans un environnement numérique doit être partagée par tous les membres du personnel et élèves du CSSD.

**6.5** Plusieurs mesures doivent être mises en place afin d'assurer une proactivité à l'égard des cybermenaces émergentes.

## 07) MODALITÉS D'APPLICATION

### 7.1 Cybercitoyenneté

- Le CSSD et l'ensemble des écoles et centres s'assurent de mettre en place des mécanismes de modération et de contrôle pour les médias numériques relevant de leur compétence. Seuls les médias numériques reconnus comme tels peuvent utiliser le nom et le logo du Centre de services scolaire des Draveurs, de l'école ou du centre.

- Le CSSD et l'ensemble des écoles et centres s'assurent de diffuser une nétiquette qui décrit les comportements à adopter en matière de cybercitoyenneté dans les médias numériques relevant de leur compétence :

  - ✓ Utiliser les actifs informationnels du CSSD de manière responsable, légale et éthique.

  - ✓ Comprendre et utiliser les médias numériques de manière responsable et éthique, comme un outil de communication, de collaboration et de partage.

  - ✓ Utiliser un français de qualité lors d'échanges.

  - ✓ Connaître son ou ses destinataires et s'y adresser de manière appropriée et respectueuse.

  - ✓ Préserver son bien-être psychologique et physique tout en faisant un usage pondéré et raisonnable des médias numériques.

  - ✓ Réagir à une situation indésirable ou menaçante en avisant les autorités compétentes.

  - ✓ Comprendre le concept de l'empreinte numérique traçable tout en saisissant l'importance de la diffusion d'une identité professionnelle qui est compatible avec les valeurs du CSSD et de l'École québécoise.

### 7.2 Cybersécurité

- Le CSSD s'assurent de mettre en place des processus formels de cybersécurité qui permettent d'assurer la gestion des risques, la gestion de l'accès aux actifs informationnels et la gestion des incidents. Pour ce faire, le CSSD, doit :
    - instaurer un processus de gestion des vulnérabilités ;
    - établir une priorité des tâches et assurer l'assignation de ressources ;
    - assurer une formation du personnel en cybersécurité.

- Le CSSD et l'ensemble des écoles et centres s'assurent de diffuser les comportements à adopter en matière de cybersécurité :

    ✓ Utiliser, dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition, en se limitant aux fins auxquelles ils sont destinés.

    ✓ Respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier leur configuration ou les désactiver.

    ✓ Signaler dès que possible à une autorité compétente tout acte qui est susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du centre de services scolaire.

## 08) <u>RESPONSABILITÉS</u>

### 8.1 Direction générale

8.1.1 S'assurer de l'application de la présente politique par l'ensemble des directions d'établissement et de service du centre de services scolaire.

### 8.2 Directions d'établissement et de service

8.2.1 S'assurer que les membres du personnel de l'unité administrative et les élèves dans le cas d'une direction d'établissement respectent les modalités d'application de la présente politique.

8.2.2 S’assure de mettre en place des mécanismes de modération et de contrôle pour les médias numériques relevant de sa compétence.

### 8.3 Responsable de la sécurité de l’information

8.3.1 Conseiller la direction générale en ce qui a trait à la détermination des orientations stratégiques et priorités d’intervention en cybersécurité ;

8.3.2 Assurer l’arrimage de toutes les préoccupations en matière de cybersécurité ;

8.3.3 Communiquer, à la demande de la direction générale, les orientations et les priorités d’intervention gouvernementales en matière de cybersécurité.

## DATE D’ENTRÉE EN VIGUEUR

La présente politique entre en vigueur dès son adoption.