



DIRECTIVE ADMINISTRATIVE

ADM.26.2

DOMAINE : **ADMINISTRATION**

En vigueur le : **25 mars 2008**

Politique :

Révisée le :

UTILISATION ACCEPTABLE DU RÉSEAU INFORMATIQUE¹

BUT :

Le Conseil scolaire de district catholique Centre-Sud permet l'accès au réseau Internet aux élèves de même qu'aux membres du personnel. Ce réseau représente une source d'information importante permettant à chacun d'accroître leur base de connaissances. L'accès au réseau encourage la recherche et l'apprentissage, il facilite l'accès à des ressources uniques et fournit l'occasion de participer à des activités éducatives collectives et coopératives.

PRINCIPES D'ÉTHIQUE INFORMATIQUE À RESPECTER :

Les élèves et les membres du personnel qui utilisent cet outil doivent respecter les principes d'éthique informatique (voir annexes ADM 26.2.1 et ADM 26.2.2).

L'utilisation du réseau est un privilège et non un droit.

Types d'utilisation acceptable :

- pour mener les affaires du Conseil;
- pour communiquer avec d'autres personnes autorisées et avec le public;
- pour recueillir les renseignements pertinents pouvant les aider dans leurs fonctions; et
- pour maîtriser les techniques d'utilisation de ce réseau.

Types d'utilisation non-acceptable :

- à des fins commerciales, pour faire la publicité de produits ou du lobbying politique;
- à des fins de divertissement (jeux de loterie, *gambling*, etc...)
- pour gêner l'usage que les autres usagers font du réseau;
- pour des fins illégales, inappropriées ou obscènes ou encore pour appuyer de telles activités.
- -Les activités illégales sont définies comme celles qui contreviennent aux lois locales, provinciales, fédérales ou criminelles. Les activités obscènes sont définies comme celles qui ont pour effet de violer les normes chrétiennes et sociales généralement acceptées.

Propriété de l'information

Cette directive administrative est conforme à la *Loi sur l'accès à l'information municipale et la protection de la vie privée* qui stipule que « toute l'information publique conservée sur papier, microfilm ou support électronique, est la propriété du Conseil ».

Le Conseil se réserve le droit d'examiner tout le matériel qui se trouve sur le compte des usagers et de superviser leurs pratiques. Toute information consignée à l'aide du réseau informatique peut faire l'objet d'une demande d'accès à l'information sous *Loi sur l'accès à l'information municipale et la protection de la vie privée*.

¹ Dans ce texte, le mot réseau englobe le réseau informatique du Conseil ainsi que l'Internet.



RESPONSABILITÉS DES USAGERS AUTORISÉS :

Il incombe aux usagers autorisés d'utiliser le réseau informatique uniquement pour les affaires du Conseil et pour les fins autorisées par le gestionnaire, comme les activités professionnelles et le perfectionnement et les utilisations personnelles autorisées.

Il importe aux usagers :

- de prendre des mesures raisonnables pour contrôler l'utilisation de leur mot de passe ;
- de se conformer aux directives destinées à assurer la sécurité du réseau informatique et de l'information qu'ils contiennent;
- d'éviter de transférer des virus informatiques dans le réseau ;
- de rédiger leurs communications de façon professionnelle (éviter d'employer des termes grossiers, abusifs ou faire des commentaires sans discernement dans leurs communications professionnelles);
- de prendre des mesures raisonnables pour s'assurer que leurs communications sur les politiques, programmes et les services sont correctes, claires et compatibles avec les politiques de leur groupe administratif ou du Conseil;
- de demander à leur superviseur de leur préciser si l'utilisation envisagée est illégale ou inacceptable, au sens de la présente directive;
- de signaler toutes activités illégales ou inacceptables.

RESPONSABILITÉ DU PERSONNEL CADRE : (direction, surintendance, direction générale)

Le personnel cadre doit informer son personnel, les parents et les tuteurs-tutrices du protocole d'utilisation du réseau informatique.

Lorsqu'une activité illégale ou inacceptable lui est signalée, un cadre peut demander une enquête après avoir consulté la personne responsable de sa supervision. Par la suite, la personne responsable de cette supervision avisera le Service de l'informatique d'autoriser son personnel à analyser les registres d'utilisation du réseau informatique, le contenu des fichiers de données et le courrier électronique et à communiquer les renseignements à la personne responsable de l'enquête.

RESPONSABILITÉS - DIRECTION D'ÉCOLE / PERSONNEL ENSEIGNANT :

Le personnel enseignant de l'école doit prendre toutes les mesures nécessaires afin d'assurer une bonne utilisation du réseau. Il est responsable de la surveillance des élèves dans les classes et les laboratoires informatiques.

L'enseignante ou l'enseignant qui permet à une ou à un élève d'accéder au réseau doit l'informer des modalités de la directive administrative, et mettre cette dernière à la disposition des parents et des tutrices ou tuteurs (par exemple, à l'aide d'une note aux parents, d'une séance d'information, d'un bulletin d'information, d'une soirée de parents, d'un comité communautaire, etc.). De plus, avant d'accorder l'accès au réseau à une ou un élève, le formulaire prévu (ADM 26.2.3) à cette fin doit être dûment rempli et conservé dans les dossiers de l'école.

Affichage des travaux d'élèves sur Internet

Pour assurer la confidentialité de l'élève, les enseignantes et enseignants doivent obtenir le consentement écrit de l'élève et d'un parent, d'une tutrice ou d'un tuteur si le nom de l'élève doit être diffusé sur l'Internet.

MESURES DISCIPLINAIRES :

En cas d'utilisation illégale ou inacceptable du réseau informatique, une mesure disciplinaire appropriée pourra être imposée par le Conseil.

Dans l'éventualité où l'utilisation illégale ou inacceptable du réseau informatique est faite par une ou un élève, des conséquences disciplinaires, pourraient être imposées par l'enseignante ou l'enseignant ou par la direction de l'école.

L'utilisation inappropriée, y compris toute violation des principes d'éthique suivants (voir annexes ADM 26.2.1 et ADM 26.2.2), peut mener à l'annulation du privilège d'accès au compte et aux accusations légales associées.