CONSEIL SCOLAIRE CATHOLIQUE NOUVELON

DIRECTIVE ADMINISTRATIVE ADM 4.3

Domaine : **Administration**

Politique : GOU 31.0 Engagement envers l'employé

En vigueur le 20 juin 2000 (SP-00-111)
Révisée le 1 juin 2021 (CF)

L'usage du masculin a pour but d'alléger le texte.

UTILISATION RESPONSABLE DU RÉSEAU INFORMATIQUE

1. ÉNONCÉ

À l'ère numérique, le Conseil scolaire catholique Nouvelon (Conseil) reconnait l'importance du réseau informatique dans sa structure de fonctionnement qui permet aux employés d'effectuer leur travail quotidien. D'une manière efficace, le réseau informatique facilite aussi les communications avec la communauté scolaire et favorise la collaboration des employés qui sont tenus d'en assurer une utilisation responsable.

2. PRINCIPES DIRECTEURS

2.1. L'utilisation du réseau informatique par les employés est un privilège et non un droit acquis.

2.2. Toute information traitée ou transmise sur le réseau est la propriété du Conseil.

2.3. L'utilisation du réseau informatique durant les heures de travail doit privilégier le travail respectif des employés.

2.4. L'employé qui choisit d'utiliser le réseau du Conseil à des fins personnelles accepte la responsabilité du risque d'atteinte à sa vie privée, c'est-à-dire qu'il perd son droit à la confidentialité des fichiers si les réseaux et ressources informatiques sont utilisés en contravention aux politiques et directives mises sur pied, ou en core à des lois ou règlements provinciaux ou fédéraux.

2.5. Le Conseil se réserve le droit de prendre les mesures nécessaires dans le cas d'une activité non permise sur le réseau.

2.6. Le Conseil ne contrôlera pas systématiquement les communications et informations des usagers. Ce contrôle aura lieu uniquement s'il y a des raisons de croire que les systèmes ont été utilisés de manière inappropriée, s'il est nécessaire de le faire pour retracer une information qui ne serait autrement disponible ou encore en application de mesures d'urgence et de sécurité; dans ce contexte, toute utilisation des ressources informatiques à des fins personnelles ne peut donc être considérée privée.

2.7. Le Conseil peut également être appelé à accéder et à produire en preuve le contenu de tout document emmagasiné dans un support informatique dans le cadre d'une procédure judiciaire.

3. DÉFINITION

Au Conseil, le réseau informatique comprend l'ensemble de l'équipement technologique, des logiciels, des applications, des sites Web, des documents et des données gérés par le Conseil. Le réseau informatique relie l'ensemble de serveurs et de postes de travail dans le but d'échanger des données, des informations et des documents de façon sécurisée. Il permet aussi l'accès à l'Internet, favorise le travail en équipe et optimise les processus, p. ex. déploiement de logiciels, installation d'imprimantes.

4. RESPONSABILITÉS

4.1. **Le Conseil :**

4.1.1. offre aux membres du personnel l'accès à son réseau informatique sécurisé;
4.1.2. précise les principes d'utilisation responsable du réseau et les activités non permises sur celui-ci;
4.1.3. met en œuvre des pratiques de gestion et de surveillance pour assurer l'utilisation responsable du réseau informatique;
4.1.4. veille au respect des diverses lois afférentes à l'informatique et l'infonuagique.

4.2. **Le Service des ressources humaines :**

4.2.1. informe les nouveaux membres du personnel de la présente directive administrative;
4.2.2. s'assure que le nouvel employé reçoive le lien à l'entente d'engagement pour qu'il atteste de son utilisation responsable du réseau informatique;
4.2.3. conserve une liste annuelle des attestations.

4.3. **Le Service de l'informatique :**

4.3.1. assure le bon fonctionnement et la sécurité du réseau informatique;
4.3.2. de façon aléatoire ou lors d'un doute raisonnable, vérifie sans préavis l'utilisation du réseau informatique d'un employé dans le but d'assurer le respect de la présente directive administrative.

4.4. **Le superviseur :**

4.4.1. revoit avec son personnel, annuellement en début d'année scolaire, les modalités de la présente directive administrative et du contrat d'engagement;
4.4.2. veille à ce que son personnel respecte la directive administrative et l'entente d'engagement;
4.4.3. en cas de manquement, prend les mesures correctives selon la directive administrative *ADM 1.12 Mesures disciplinaires pour comportement fautif*.

4.5. **Le membre du personnel :**

4.5.1. s'engage à attester d'avoir lu et compris l'entente d'engagement;
4.5.2. respecte la présente directive administrative et l'entente d'engagement.

5. ACTIVITÉS NON PERMISES SUR LE RÉSEAU INFORMATIQUE

5.1. Il est interdit d'utiliser le réseau informatique en fonction d'activités non autorisées ou illégales. Voici une liste non exhaustive des activités non autorisées :

5.1.1. la diffusion d'information, la sollicitation ou la publicité qui va à l'encontre de la mission et des vertus du Conseil;
5.1.2. la transmission, la réception, la reproduction, la distribution ou la sauvegarde de matériel protégé par les droits d'auteur, les droits de propriété intellectuelle, et tout matériel illégal;
5.1.3. le téléchargement, l'installation, l'utilisation ou la transmission de logiciels piratés ou illicite;
5.1.4. l'installation, l'utilisation, la reproduction et la transmission d'un logiciel piraté;
5.1.5. la diffusion non autorisée de renseignements personnels pouvant porter atteinte à la vie privée, p. ex. nom, adresse, numéro de téléphone, photos, vidéos;
5.1.6. des actes visant à porter atteinte à l'intégrité ou à la confidentialité des données de d'autres usagers ou organismes;
5.1.7. toute forme de cyberintimidation, de harcèlement, de menace, de diffamation, d'injures ou de traque;
5.1.8. l'utilisation de l'identité d'un autre usager;
5.1.9. le téléchargement, la consultation, la transmission, l'affichage, la publication, la diffusion, la réception, la récupération et la conservation de contenu de nature haineuse, violente, diffamatoire, abusive, obscène, profane, pornographique, menaçante, dénigrante ou à caractère discriminatoire basé sur la race, la couleur, le sexe, l'orientation sexuelle, l'état civil, la religion, la langue, l'origine ethnique, la condition sociale ou un handicap quelconque;
5.1.10. des actes visant à endommager ou à détruire du matériel;
5.1.11. des actes qui risquent de perturber le réseau informatique;
5.1.12. toutes activités commerciales ou politiques;
5.1.13. la transmission d'un message électronique de façon anonyme ou en utilisant le nom d'une autre personne;
5.1.14. l'accès, la sauvegarde ou la distribution de matériel et de sites Web jugés inappropriés;
5.1.15. des actes pouvant nuire à la réputation du Conseil, de ses écoles ou d'une personne;
5.1.16. la participation à des jeux à l'Internet, sauf s'il s'agit d'une activité pédagogique supervisée qui respecte les mesures de sécurité de l'utilisation du réseau informatique;
5.1.17. l'insertion ou la propagation de virus informatiques;
5.1.18. des actes visant à désactiver, à endommager, à détruire ou à contourner les mesures de sécurité.

6. RÉFÉRENCES

6.1. Charte canadienne des droits et libertés (L.C. 1982)

6.2. *Loi sur la protection des renseignements personnels* (L.R.C., 1985, ch. P-21)

6.3. *Loi sur les droits d'auteur* (L.R.Cl, 1985, c.C-42)

6.4. Code criminel (L.R.C., 1985, c. C-46)

6.5. *Loi sur l'éducation* (L.R.O., 1990, ch. E.2)

6.6. *Loi sur l'accès à l'information* (L.R.C., 1985, ch.A-1)

6.7. Loi sur l'accès à l'information municipale et la protection de la vie privée

6.8. (L.R.O. 1990, M.56)

6.9. Projet de loi 14, *Loi sur la lutte contre l'intimidation*