TIC-01 : Utilisation responsable des technologies de l'information et des communications	EN VIGUEUR : 2024-09-24 RÉVISÉE LE :

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 3.6 portant sur la protection des actifs et, à ce titre, fait l'objet d'un rapport annuel de monitoring.

Cette directive administrative fait état des éléments suivants :

- Encadrement de l'utilisation de l'équipement informatique et des outils technologiques liés aux technologies de l'information et des communications (TIC) à l'école, sur la propriété de l'école et toutes autres propriétés du Conseil ainsi que dans les endroits où l'équipement et les services informatiques du Conseil scolaire catholique des Grandes Rivières (le CSCDGR) sont utilisés, par exemple, à la maison.
- Précisions sur les attentes quant à l'utilisation sécuritaire et responsable des réseaux informatiques liés aux TIC du CSCDGR pour tout utilisateur qui se sert, pour une quelconque raison, des réseaux et des ressources informatiques du CSCDGR.
- Exigences de l'assureur du Conseil, Ontario School Board's Insurance Exchange (OSBIE) en mettant en place un ensemble de critères auxquels le CSCDGR adhère pour garantir une protection optimale de nos élèves, de notre personnel et de nos biens, tout en minimisant les risques et les responsabilités potentielles auxquels le CSCDGR pourrait être exposé.

DESTINATAIRES

La présente directive administrative s'adresse à l'ensemble des utilisateurs des technologies du CSCDGR, soit le personnel, les élèves, les travailleurs indépendants, les conseillères et conseillers scolaires, ainsi que toute autre personne faisant usage de ces ressources. Cela inclut les visiteurs et les membres de la communauté qui interagissent avec les technologies du CSCDGR.

DÉFINITIONS

Accès : S'entend de l'entrée en communication avec un réseau informatique que le CSCDGR a mis à la disposition des personnes autorisées. L'accès à un tel réseau peut avoir lieu dans les locaux mêmes du CSCDGR ou à l'extérieur de ceux-ci. L'accès peut

également comprendre les personnes autorisées utilisant les réseaux informatiques fournis par le CSCDGR à des fins personnelles.

Activité illégale : S'entend des actes criminels, des infractions à des lois fédérales et provinciales non pénales à caractère réglementaire ainsi que des actions qui rendent une personne autorisée ou un établissement passible de poursuites.

Activité inacceptable : S'entend de toute activité contraire aux lois, règlements et aux directives administratives du CSCDGR, au code de conduite provincial de l'Ontario, au code de conduite des écoles et aux normes professionnelles applicables au personnel.

Appareil mobile personnel : S'entend de tout appareil électronique personnel pouvant être utilisé pour communiquer ou accéder à Internet, tel un téléphone portable, une tablette, un ordinateur portable ou une montre intelligente.

Authentification multifacteur : Authentification qui met en œuvre, de façon simultanée, des procédés de vérification faisant appel à au moins deux facteurs d'authentification différents.

Citoyenneté numérique : S'entend de la participation active de l'individu dans une société numérique, tout en étant responsable pour ses actions, en suivant des normes de conduite et une procédure, et en assurant la sécurité ainsi que le bien-être psychologique de soi et des autres. (Réf. : Annexe 1 – Principes de citoyenneté numérique)

Environnement infonuagique : S'entend d'un environnement informatique virtuel qui vise la gestion des données informatiques et le stockage des informations. Celui-ci permet, au moyen de serveurs distants interconnectés par Internet, un accès à des ressources informatiques pouvant être partagées et configurables.

Néthique et nétiquette : S'entend des règles de conduite à caractère moral, les règles de politesse et de savoir-vivre que doivent emprunter les utilisateurs des TIC (annexe 2). Les actes illégaux posés lors de l'utilisation des TIC qui contreviennent à l'éthique sont, par exemple et sans s'y limiter, le piratage, la violation de données, l'atteinte aux droits d'auteur, la diffusion de documents illicites, toute atteinte au droit de la vie privée, entre autres à caractère pornographique ou à la propagande haineuse. Ces situations peuvent être considérées comme de la criminalité informatique.

Médias ou réseaux sociaux numériques : S'entend de tous les médias permettant la création, le partage et l'échange virtuels de contenu et d'idées entre individus. Il s'agit, entre autres, de blogues, de sites Internet personnels, de flux RSS et de messages affichés sur des sites variés.

Personnes autorisées : S'entend des personnes à qui il est permis d'utiliser les réseaux sécurisés et les outils ou appareils numériques fournis et gérés par le CSCDGR.

Plan de citoyenneté numérique : S'entend d'un plan élaboré par l'équipe école, en consultation avec le conseil d'école, à partir du plan générique fourni par le CSCDGR.

Réseau informatique : S'entend d'un groupe d'ordinateurs et de systèmes informatiques capables de communiquer ensemble.

Service des technologies de l'information : S'entend comme étant le service administratif relevant de la direction de l'éducation et secrétaire-trésorier qui est responsable de la mise en œuvre de la présente directive administrative.

Sites non autorisés : S'entend de sites Internet qui ont été bloqués par le CSCDGR pour une des raisons suivantes : les sites portent atteinte à la sécurité des élèves et du personnel; les sites sont opposés aux valeurs morales prônées par le CSCDGR; les sites sont jugés inappropriés en raison de l'âge de l'utilisateur; les sites compromettent la confidentialité des renseignements personnels des élèves et du personnel du CSCDGR; tout site Internet pouvant endommager, compromettre, violer, infiltrer ou pouvant nuire aux ordinateurs, aux appareils numériques, aux réseaux et aux ressources informatiques du CSCDGR ou à ceux des autres utilisateurs.

Technologies de l'information et des communications (TIC) : S'entend de l'ensemble de l'équipement informatique et des ressources technologiques permettant de transmettre, de copier, de créer, de modifier, de partager ou d'échanger des informations, y compris, sans s'y limiter : les serveurs, les réseaux, les appareils numériques tels les ordinateurs, les tablettes, les téléphones intelligents, les accessoires périphériques de lecture, d'emmagasinage, de copie, d'impression, de transmission, de réception et de traitement de l'information, ainsi que les services multimédias et audiovisuels.

Utilisateur : S'entend de toute personne qui utilise, pour une quelconque raison, les réseaux et les ressources informatiques du CSCDGR, telle les élèves, les membres du personnel, les bénévoles, les parents, les visiteurs.

MODALITÉS D'APPLICATION

1. Conformément à la Politique/Programme Note 128, les membres de la communauté scolaire ne doivent pas utiliser d'appareils mobiles personnels pendant les heures de travail, sauf exceptions (voir directive administrative TIC-02).
2. Le CSCDGR reconnaît les bénéfices pédagogiques et pratiques de permettre l'utilisation des systèmes informatiques, incluant l'accès aux divers outils technologiques et à Internet pour les utilisateurs, tout en veillant à la sécurité, à la protection des données et au respect mutuel entre utilisateurs. Le CSCDGR établit des modalités concernant l'utilisation du parc informatique au sein du CSCDGR.
3. Chaque utilisateur est responsable des actions effectuées lors de son utilisation des divers outils technologiques et du réseau informatique.
4. Tous les utilisateurs doivent adhérer aux valeurs promues par le CSCDGR.
5. L'utilisation doit se faire dans le respect des normes de conduite établies, de la confidentialité des données et des règles d'accès aux ressources numériques.
6. L'utilisateur doit respecter les critères de sécurité et s'assurer de ne pas partager les informations confidentielles avec des utilisateurs non autorisés.
7. Il est impératif de signaler sans délai tout incident de sécurité, toute infraction ou tout comportement inapproprié en lien avec l'utilisation du parc informatique.
8. Les incidents informatiques sont évalués et traités rapidement et de manière appropriée.
9. Un filtrage des contenus Web est mis en place pour réglementer l'accès à Internet; bien que le CSCDGR s'efforce de gérer efficacement ces accès, des dérogations imprévues peuvent survenir.

10. Les utilisateurs doivent se limiter à des activités éducatives, pédagogiques ou administratives du Conseil.
11. Les utilisateurs doivent être conscients que le CSCDGR est autorisé à examiner l'historique d'utilisation des appareils, de navigation Internet, et des comptes du Conseil.
12. Tous les utilisateurs qui tentent de contourner la sécurité établie par le CSCDGR auront leurs accès au système informatique révoqués et des mesures disciplinaires ou légales s'appliqueront.
13. Les appareils à risque ou infectés peuvent être restreints ou exclus du réseau pour préserver sa sécurité.
14. Tout outil ou logiciel utilisé dont la fonction vise à perturber le parc informatique est strictement interdit au CSCDGR.

PROCESSUS

1. CONDITIONS D'UTILISATION DES TIC

1.1 Utilisation responsable des TIC

1.1.1 Chaque utilisateur des TIC du CSCDGR est tenu de se servir de son accès de façon judicieuse. Il doit respecter la présente directive et toute autre directive administrative connexe du CSCDGR ainsi que les lois et les règles s'y rattachant. En cas de doute, l'utilisateur doit demander à sa superviseure, son superviseur immédiat, au Service informatique du CSCDGR, à la direction ou à une enseignante, un enseignant pour ce qui est des élèves, de lui préciser si l'utilisation envisagée est illégale ou inacceptable, selon les modalités des directives administratives en vigueur.

1.2 Privilège et droit d'accès

1.2.1 L'utilisation des TIC du CSCDGR est un privilège accordé aux utilisateurs autorisés qui acceptent de les utiliser de façon responsable et sécuritaire. Ce privilège peut être révoqué si l'utilisateur ne se conforme pas à la présente directive. De plus, selon les actions posées, le CSCDGR peut avoir recours à diverses mesures disciplinaires telles que celles précisées à l'article 16 de la présente directive administrative.

1.2.2 Seules les personnes autorisées peuvent avoir accès aux TIC du CSCDGR. Un utilisateur autorisé ne peut permettre qu'un tiers non autorisé utilise les TIC du CSCDGR.

1.3 Règles d'utilisation

1.3.1 Les TIC doivent être utilisées à des fins professionnelles, administratives, pédagogiques et scolaires relativement à la mission, à la vision et aux valeurs du CSCDGR.

1.3.2 Les communications se font en français, sauf exception lorsque l'utilisateur communique avec des parents ou des organismes ne pouvant pas communiquer en français ou dans le cadre d'un cours de langue autre que le français. Les

ressources, le matériel et les sites en français sont à privilégier lors de l'utilisation des TIC.

1.4 Utilisation des TIC à des fins personnelles par les membres du personnel

1.4.1 L'utilisation personnelle sera tolérée dans la mesure où les conditions suivantes sont respectées :

- L'utilisation des TIC est effectuée hors des heures de travail ou à un temps où l'utilisation n'interfère pas avec le travail de l'employé ou celui des autres employés (Par exemple : à l'heure du dîner, à une pause);
- l'utilisation ne nuit pas au fonctionnement optimal des TIC;
- l'utilisation n'entraîne pas de coût supplémentaire;
- l'utilisation ne sert pas à des fins commerciales, lucratives, de propagande ou illégales.

1.4.2 En cas d'abus, le CSCDGR a le droit de retirer ou de limiter ce privilège.

1.4.3 Le Conseil décline toute responsabilité en cas d'utilisation d'informations personnelles sur les TIC du Conseil. (Par exemple : Stockage de données personnelles financières, utilisation de comptes personnels, etc.)

1.5 Accès et mots de passe

1.5.1 L'utilisateur est responsable de la confidentialité et de l'usage du code d'accès et du mot de passe qui lui sont attribués pour accéder aux TIC. L'utilisateur est responsable de tout acte provenant de son compte; ainsi, il est important de protéger son code d'accès et son mot de passe. En conséquence, il faut choisir un mot de passe « fort » et le modifier selon les normes exigées par le logiciel utilisé.

1.5.2 L'utilisateur doit utiliser une authentification multifacteur pour les applications auxquelles ce niveau de sécurité est exigé.

1.5.3 Il est interdit d'utiliser le code d'accès ou le mot de passe d'un autre utilisateur. Si le code d'accès ou le mot de passe est perdu ou s'il y a raison de croire que le compte est compromis, la personne désignée sera avisée et un nouveau mot de passe sera créé.

1.6 Courriel

1.6.1 Pour tout courriel diffusé sur le réseau du CSCDGR, l'utilisateur doit s'identifier à titre de signataire de son message.

1.6.2 Tout courriel ou autres communications diffusés à titre de parent doivent être émis par l'entremise d'un abonnement personnel. (gmail.com, Outlook.com)

1.6.3 L'utilisateur doit respecter la confidentialité des messages transmis sur le réseau et s'abstenir d'intercepter, de lire, de modifier ou de détruire tout message qui ne lui est pas destiné.

1.6.4 Comme pour toute autre forme de communication qui se prévaut des TIC (Par exemple : forum de discussion, clavardage), l'utilisateur doit communiquer de

façon respectueuse et professionnelle en respectant les règles de l'étiquette (Annexe 2).

1.7 Communications

1.7.1 L'utilisateur doit s'assurer que ses communications sont empreintes de respect et de civisme, et qu'elles sont rédigées dans un langage courtois, et ce, pour éviter que son utilisation des TIC ternisse la réputation de l'école, du CSCDGR ou de la communauté scolaire.

1.7.2 L'utilisateur doit prendre des mesures raisonnables pour s'assurer que ses communications sur les directives, les programmes et les services du CSCDGR représentent correctement l'intention du CSCDGR.

1.8 Confidentialité de l'information

1.8.1 L'utilisateur est responsable de prendre les mesures nécessaires pour protéger la confidentialité des informations sous sa responsabilité. Il doit respecter la *Loi sur l'accès à l'information municipale et la protection de la vie privée* en ce qui a trait à la conservation, à l'accès, à la transmission et à la diffusion des données et des renseignements personnels.

1.8.2 L'utilisateur doit s'abstenir de partager des renseignements personnels au sujet des autres personnes sans leur autorisation. Ces renseignements peuvent prendre la forme d'information écrite, de photos ou d'autres documents visuels où les personnes peuvent être identifiées de façon nominative.

1.8.3 L'utilisateur doit prendre toutes les mesures raisonnables pour protéger les copies de travail de documents qui contiennent des renseignements personnels, dont l'utilisation de mots de passe ou cryptage et un contrôle accru des accès.

1.8.4 Afin de préserver la confidentialité des renseignements personnels, il est impératif de supprimer ou de détruire de manière sécurisée tout document contenant ces informations dès que son utilisation n'est plus nécessaire.

1.8.5 Il est interdit de sauvegarder des documents contenant des informations personnelles sur des médias amovibles (par exemple des clés USB).

1.8.6 Il est interdit de sauvegarder des documents contenant des informations personnelles sur des équipements personnelles (AVAN).

1.8.7 Il est interdit de sauvegarder des documents contenant des informations personnelles sur des plateformes infonuagiques autres que celles fournies par le CSCDGR.

1.9 Droit d'auteur et propriété intellectuelle

1.9.1 L'utilisateur doit respecter les lois qui protègent les droits d'auteur et les droits de propriété intellectuelle. Les reproductions de logiciels de documents numérisés ou de service Web doivent se faire selon les conditions de la licence d'utilisation qui les régit.

2. UTILISATION SÉCURITAIRE DES TIC

2.1 L'utilisateur est responsable de se renseigner au sujet des questions relatives à la sécurité des TIC. Il doit s'abstenir :

- De poser des actes qui nuisent au bon fonctionnement des TIC (Par exemple : transférer des virus informatiques sur les réseaux);
- d'en faire une utilisation qui aurait pour effet d'en diminuer le rendement, d'en limiter l'accès ou d'en interrompre le fonctionnement (Par exemple : effectuer un stockage abusif d'informations, utilisation immodérée d'un service de diffusion en ligne);
- d'accéder à des fichiers, à des ressources, à du contenu ou à des sites Web non autorisés dont l'accès est limité à une catégorie spécifique d'usagers ou qui risquent d'endommager, de compromettre, d'infiltrer ou de nuire aux TIC du CSCDGR;
- de désactiver ou de contourner intentionnellement les systèmes de sécurité;
- d'effacer les indices d'activités douteuses ou illégales;
- de modifier ou de détruire des données, des logiciels ou toutes autres ressources informatiques sans l'approbation de l'autorité compétente;
- de contourner les filtres Internet et les pares-feux établis par le Service informatique du CSCDGR;
- d'encourager tout autre individu à adopter un comportement prohibé.

2.2 À la suite d'une observation d'un problème potentiel de sécurité, l'utilisateur a la responsabilité d'informer soit sa superviseure, son superviseur immédiat, la direction de l'école ou un membre du Service informatique afin que la situation soit rapportée au Service informatique.

2.3 Le CSCDGR décline toute responsabilité, directe ou indirecte, à l'égard de pertes, dommages ou inconvénients subis par les utilisateurs suivant l'utilisation des TIC, ou résultant d'une réduction ou interruption des services, quelle que soit leur durée ou leur raison.

3. UTILISATION RESPONSABLE D'UN APPAREIL NUMÉRIQUE PERSONNEL – APPORTEZ VOTRE APPAREIL NUMÉRIQUE (AVAN)

Le CSCDGR reconnaît que l'utilisation d'appareils personnels sur le réseau du CSCDGR peut offrir des avantages pédagogiques et pratiques. Cependant, pour garantir la sécurité du réseau et la protection des données, le CSCDGR établit des modalités concernant l'utilisation d'appareils personnels au sein du CSCDGR.

3.1 En conformité avec la directive ministérielle PPN 128, aucun membre de la communauté scolaire ne doit utiliser d'appareils mobiles personnels pendant les heures d'enseignement ou de travail, sauf dans les circonstances suivantes :

a) À des fins éducatives, selon les directives d'un membre du personnel enseignant
b) À des fins sanitaires et médicales
c) Pour répondre à des besoins éducatifs spéciaux
d) En cas d'urgence pour demander de l'aide

3.2 Les utilisateurs autorisés doivent adhérer aux consignes de sécurité établies par le CSCDGR.

3.3 L'utilisation des ressources infonuagiques du CSCDGR est sujette à des mesures de sécurité additionnelles.

3.4 Le CSCDGR ne fournira aucune assistance technique pour les appareils personnels des utilisateurs.

3.5 Les utilisateurs doivent assurer eux-mêmes la maintenance et le bon fonctionnement de leurs appareils personnels.

3.6 La sécurité des appareils personnels, incluant la protection contre les virus, les logiciels malveillants et l'application des correctifs de sécurité, incombe à chaque utilisateur.

3.7 Le réseau destiné aux appareils personnels est isolé des réseaux critiques du CSCDGR afin de réduire les risques de sécurité.

3.8 La transmission d'informations confidentielles ou sensibles doit être évitée. Le CSCDGR ne peut pas assurer ou se porter responsable de la confidentialité de tout renseignement que l'utilisateur transmet au moyen du réseau sans fil.

3.9 Les appareils numériques personnels ne doivent pas être branchés sur le réseau filaire, aux stations d'accueil dans les classes ou les bureaux du CSCDGR; seul le réseau sans fil conçu pour les appareils personnels peut être utilisé.

3.10 Toute personne qui apporte un appareil numérique personnel (ordinateur, tablette ou téléphone cellulaire) sur les lieux du CSCDGR ou dans les écoles doit :

- Prendre les mesures nécessaires pour assurer que l'appareil numérique personnel ne puisse nuire au fonctionnement du parc informatique du CSCDGR;
- savoir utiliser, gérer et sécuriser l'appareil numérique personnel dans son milieu de travail, conformément à la présente directive administrative;
- assumer la responsabilité en cas de perte, vol ou endommagement du dispositif. Le CSCDGR n'est pas responsable des appareils numériques personnels.

4. UTILISATION DES LOGICIELS

Les logiciels constituent une composante cruciale des opérations pédagogiques et administratives au sein du CSCDGR. Pour assurer leur utilisation adéquate, sécurisée, légale et efficace, le Service informatique se charge du suivi et de l'évaluation des risques en matière de cybersécurité et de la vie privée. Le CSCDGR établit des modalités sur l'emploi des logiciels au CSCDGR :

4.1 Tous les logiciels et les abonnements exploités doivent être acquis dans le respect de la réglementation, munis de licences valides et utilisés en accord avec les conditions des accords de licence.

4.2 La gestion des licences et la vérification de la conformité relèvent de la responsabilité du Service informatique.

4.3 L'utilisation de systèmes d'exploitation et de logiciels doit être légitime, respecter les accords de licence et doit activement recevoir les correctifs et mises à jour de sécurité.

4.4 Seul le personnel dûment autorisé est habilité à installer des logiciels sur l'équipement informatique du CSCDGR.

4.5 Les mises à jour de sécurité sont effectuées et les correctifs sont mis en œuvre de manière systémique afin d'assurer la sécurité et la stabilité des systèmes.

4.6 La responsabilité de la gestion des mises à jour incombe aux administrateurs de systèmes, soit le CSCDGR ou un organisme tiers.

4.7 Chaque utilisateur des logiciels du CSCDGR doit adhérer aux principes de sécurité, de confidentialité et d'accès autorisé.

4.8 L'accès aux logiciels jugés critiques ou sensibles sera restreint aux utilisateurs ayant reçu une autorisation.

4.9 Des sessions de formation sur l'usage approprié des logiciels et sur la sensibilisation à la cybersécurité seront offertes ou même exigées.

5. STANDARDISATION DES OUTILS INFORMATIQUES

Le CSCDGR s'engage à offrir un cadre informatique sécurisé, performant et fiable pour appuyer les activités éducatives et administratives visant à assurer leur cohérence, leur sécurité et leur compatibilité. Le CSCDGR établit des modalités concernant les standards des outils informatiques au CSCDGR.

5.1 L'équipement informatique (ordinateurs, tablettes, etc.) doit répondre aux spécifications minimales fixées par le CSCDGR pour garantir une performance optimale.

5.2 Les ordinateurs et les serveurs du Conseil doivent être préparés avec une configuration prédéterminée afin de réduire les risques de cyberattaque.

5.3 L'équipement doit être maintenu en parfait état de fonctionnement et faire l'objet de maintenances régulières.

5.4 Le secteur informatique effectue le déploiement des mises à jour de sécurité et des correctifs de manière systémique.

5.5 L'utilisateur est responsable d'accepter la mise à jour poussée à son appareil ou d'informer le secteur informatique si les mises à jour cessent de s'installer.

5.6 Les solutions informatiques doivent répondre aux exigences des programmes éducatifs et aux besoins administratifs du Conseil.

5.7 La compatibilité des systèmes en place est essentielle pour tous les outils.

5.8 Les mesures de sécurité des données doivent être respectées pour assurer la confidentialité et l'intégrité des informations confidentielles.

5.9 Le chiffrement et les contrôles d'accès doivent être mis en œuvre si possible.

5.10 L'accessibilité aux outils doit être assurée, en accord avec les législations et règlementation applicable.

5.11 Des formations doivent être organisées pour permettre une utilisation optimale des ressources informatiques par les utilisateurs.

5.12 Une assistance technique doit être accessible pour aider à résoudre les problèmes et répondre aux interrogations des utilisateurs.

5.13 L'introduction de nouveaux outils informatiques nécessite une évaluation préalable pour vérifier leur adéquation avec les standards et exigences en vigueur.

5.14 Des vérifications de sécurité et de conformité sont effectuées régulièrement pour assurer la sécurité du parc informatique.

5.15 Les correctifs de vulnérabilité sont mis en œuvre selon les meilleures pratiques.

6. GESTION DES COMPTES INFORMATIQUES

La gestion des comptes informatiques est un élément essentiel de la sécurité des systèmes d'information. Le CSCDGR établit des modalités concernant les règles et la procédure pour la création, la gestion et la sécurité des comptes informatiques, garantissant ainsi la protection des données et la confidentialité des informations au CSCDGR.

6.1 Les comptes informatiques ne seront créés que pour les membres du personnel, les entrepreneurs et les élèves autorisés.

6.2 Toute création de comptes doit être effectuée par un administrateur de système dûment autorisé.

6.3 Les comptes multi-utilisateurs (partagés) ne sont pas permis.

6.4 Les mots de passe ne doivent pas être synchronisés/harmonisés/identiques pour une plage d'utilisateurs.

6.5 L'identité numérique (nom d'utilisateur et mot de passe) doit être traitée de manière confidentielle. Si le mot de passe d'un utilisateur est divulgué, celui-ci doit être changé.

6.6 Seules les personnes autorisées peuvent modifier le mot de passe d'un autre utilisateur.

6.7 L'utilisateur est responsable de verrouiller sa session à l'ordinateur s'il n'est pas en mesure d'en assurer le monitorage.

6.8 Les mots de passe doivent être conformes aux normes établies par le CSCDGR et entreposés dans un endroit sécuritaire et confidentiel.

6.9 Tous les membres du personnel qui possèdent un compte conseil doivent utiliser la fonction d'authentification multifacteur.

6.10 Les autres comptes d'utilisateur pourraient être soumis à l'utilisation de l'authentification multifacteur.

6.11 Les comptes inactifs sont régulièrement examinés et des mesures sont prises pour désactiver ou supprimer les comptes qui ne sont plus nécessaires.

6.12 Les utilisateurs sont responsables de toutes les activités associées à leur compte informatique.

7. GESTION DES CONTRÔLES D'AUTHENTIFICATION ET D'AUTORISATION

La gestion des contrôles des authentifications et des autorisations est d'une importance cruciale pour la sécurité et la gestion des accès. Le CSCDGR établit des modalités concernant la gestion des contrôles d'authentification et d'autorisation au CSCDGR.

7.1 L'accès aux ressources, y compris les applications et les données, est réglementé pour assurer une utilisation appropriée et sécuritaire.

7.2 L'accès aux ressources du CSCDGR est géré en utilisant le principe du moindre privilège.

7.3 L'accès à des ressources sensibles ou confidentielles sera strictement limité aux individus dûment autorisés.

7.4 Un gestionnaire de mot de passe doit être utilisé selon le type de poste occupé.

7.5 Les accès aux identifiants entreposés dans le gestionnaire de mots de passe sont contrôlés en utilisant le principe du moindre privilège.

7.6 Les administrateurs système et les utilisateurs sont formés sur l'importance de la sécurité des contrôles.

7.7 L'utilisation hors du pays d'un compte conseil est assujettie à des restrictions.

8. GESTION ET ÉVALUATION DE LA CYBERSÉCURITÉ

La sécurité des données est une priorité absolue au sein du CSCDGR. Dans un environnement de plus en plus infonuagique, il est essentiel de mettre en place une procédure et des contrôles pour évaluer et assurer la cybersécurité pour l'ensemble du Conseil. Le CSCDGR établit des modalités concernant la gestion et l'évaluation de la cybersécurité au CSCDGR.

8.1 Une évaluation complète des risques liés à la cybersécurité sera effectuée pour chaque ressource informatisée.

8.2 Les journaux d'évènements du parc informatique sont conservés à des fins d'analyse.

8.3 Les risques sont classés en fonction de leur gravité et de leur effet sur la cybersécurité au CSCDGR.

8.4 Les analyses de cybersécurité sont réalisées de façon continue pour garantir la conformité des systèmes informatiques.

8.5 Les contrôles techniques sont périodiquement évalués et ajustés pour répondre aux évolutions des menaces.

8.6 Les droits d'utilisateur sont régulièrement évalués et ajustés pour éviter l'accumulation de privilèges.

8.7 Un plan de gestion des incidents de cybersécurité est élaboré et maintenu par le CSCDGR.

8.8 Afin de sensibiliser les utilisateurs, le CSCDGR effectuera un minimum de trois campagnes de sensibilisations annuellement portant sur les risques d'hameçonnage.

8.9 Le CSCDGR applique le principe « confiance zéro » pour gérer l'architecture informatique.

9. GESTION DES TIERS INFORMATIQUES

Le CSCDGR reconnaît l'importance croissante des services informatiques fournis par des tiers pour soutenir les opérations éducatives et administratives. Afin d'assurer la sécurité des données, la confidentialité et la conformité, le CSCDGR établit les règles et la procédure pour la gestion des tiers informatiques au sein du Conseil.

9.1 Les tiers informatiques font périodiquement l'objet d'une évaluation complète de la sécurité, de la conformité et de la réputation du fournisseur.

9.2 Tous les tiers informatiques sont liés par des contrats ou des accords de service précisant les responsabilités en matière de sécurité des données, de confidentialité, de disponibilité et de conformité.

9.3 Le CSCDGR doit s'assurer que les données stockées ou traitées par les tiers informatiques sont gérées de façon sécuritaire.

9.4 Le CSCDGR exige des critères de sécurité élevés pour que les tiers aient accès à une ressource du parc informatique.

9.5 L'accès aux données stockées ou traitées par les tiers informatiques doit être restreint aux personnes autorisées.

9.6 Les autorisations d'accès doivent être régulièrement évaluées et mises à jour en fonction des besoins.

9.7 Les incidents doivent être signalés, évalués et traités rapidement et de manière appropriée en collaboration avec le tiers infonuagique.

10. GESTION DES RISQUES

10.1 Le personnel TIC du CSCDGR s'engage à fournir un niveau raisonnable de filtrage dans l'accès au contenu sur Internet. Le CSCDGR reconnaît qu'il est impossible de contrôler entièrement l'information à laquelle l'utilisateur peut accéder au moyen d'Internet. Certains produits, contenus ou services offerts pourraient ne pas convenir à l'utilisateur ou ne pas respecter la réglementation applicable.

10.2 Le CSCDGR n'assume aucune responsabilité pour toute réclamation, tout préjudice étant associé ou découlant de l'accès ou de l'utilisation des contenus.

11. VÉRIFICATION DE L'UTILISATION

11.1 Le CSCDGR peut effectuer une vérification de l'utilisation des TIC afin d'en assurer le bon fonctionnement. Ainsi, les utilisateurs ne peuvent pas raisonnablement s'attendre à ce que leur utilisation des TIC soit privée. Le CSCDGR peut intercepter, accéder, extraire, lire, divulguer et utiliser toute communication et activité en ligne, y compris l'accès à Internet et aux courriels, pour les raisons suivantes et non limitées à celles-ci :

- Surveiller l'utilisation d'un utilisateur durant les heures de travail ou lors de l'utilisation des systèmes du CSCDGR;
- effectuer une analyse de cybersécurité;
- effectuer l'entretien ou des réparations;
- analyser les tendances d'utilisation du réseau et des logiciels;
- enquêter sur une violation d'un contrat d'emploi, d'une politique, d'une directive administrative ou d'une convention collective;
- répondre à une demande de divulgation conformément à une loi ou un règlement ou à une ordonnance d'un tribunal compétent, y compris lorsqu'il est question d'une enquête informatique;
- assurer la continuité des opérations;
- améliorer les processus des activités et gérer la productivité;
- prévenir les mauvais comportements et s'assurer de la conformité aux lois et règlements, aux politiques et aux directives administratives du CSCDGR et aux attentes d'ordre éthique et professionnel.

11.2 Tout document numérique, programme, média, ainsi que l'accès aux réseaux qui est emmagasiné, transmis, diffusé sur l'équipement informatique, les lieux, les réseaux ou les ressources numériques du CSCDGR peuvent être assujettis à une révision ou à un examen approfondi par le CSCDGR.

12. UTILISATION INACCEPTABLE DES TIC

12.1 Il est interdit d'utiliser les TIC, un appareil numérique personnel ou le réseau sans fil du CSCDGR pour des activités non autorisées ou illégales. Ces activités peuvent comprendre, sans s'y limiter :

- 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;
- le téléchargement ou l'installation des logiciels ou d'application sur les outils du CSCDGR, y compris ceux offerts gratuitement sur Internet ou ailleurs, sans l'autorisation du Service informatique du CSCDGR;
- l'installation, l'utilisation et la transmission de toute reproduction illicite d'un logiciel;
- la diffusion non autorisée de renseignements personnels (renseignements nominatifs tels un nom, une adresse, un numéro de téléphone personnel, des photographies, des vidéos);

- des actes visant à porter atteinte à l'intégrité ou à la confidentialité des données d'autres utilisateurs ou d'autres organismes;
- toute forme de cyberintimidation, de harcèlement, de menace, de diffamation, d'injures, de traque ou toute autre violation des droits légaux;
- l'usurpation de l'identité d'un autre usager;
- le téléchargement ou le téléversement, 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;
    - qui viole toute loi ou règlement de l'Ontario, du Canada ou d'une autre juridiction;
- l'utilisation d'appareil numérique avec des fonctions d'appareil photo, vidéo ou audio dans les endroits où il y a une attente raisonnable relative au droit à la vie privée et à la dignité d'une personne (ex. : toilettes, vestiaires);
- des actes visant à endommager ou à détruire du matériel;
- des actes qui risquent de perturber les réseaux;
- toute activité commerciale ou politique;
- la diffusion d'information, la sollicitation ou la publicité incompatible avec la mission du CSCDGR et de l'école;
- la transmission d'un message électronique de façon anonyme ou en utilisant le nom d'un autre utilisateur;
- la transmission de courriels en chaîne;
- l'accès, la sauvegarde ou la distribution de matériel et de sites Web jugés inappropriés;
- des actes pouvant nuire à la réputation du CSCDGR, de ses écoles ou d'une personne;
- la participation à des jeux sur Internet, sauf s'il s'agit d'une activité pédagogique supervisée qui respecte les mesures de sécurité de l'utilisation des TIC;
- l'abonnement à des listes d'envoi n'ayant aucun lien avec la fonction de l'utilisateur;
- l'insertion ou la propagation de virus informatiques;
- des actes visant à désactiver, à endommager, à détruire ou à contourner les mesures de sécurité;
- des actes visant à surcharger la bande passante par une utilisation exagérée;
- des actes qui entraînent des frais d'utilisation supplémentaires;
- la participation à des activités de piratage;
- altérations des outils du Conseil (par exemple : un autocollant, un graffiti, une engravure)

12.2 Les exemples d'utilisation inacceptable susmentionnés visent à démontrer l'intention du CSCDGR en ce qui a trait aux comportements des utilisateurs. Il ne s'agit pas d'une liste exhaustive. L'utilisateur a la responsabilité de reconnaître et de respecter l'intention qui sous-tend la présente directive administrative. L'utilisateur doit éviter l'utilisation de moyens pour porter atteinte au fonctionnement des TIC, même si ces moyens ne sont pas précisés dans la présente directive.

12.3 S'il y a connaissance d'activités illégales ou inacceptables de la part d'autres utilisateurs, l'utilisateur a la responsabilité d'informer soit sa superviseure, son superviseur immédiat, la direction de l'école ou un membre du personnel afin que le Service informatique soit informé.

13. MÉDIAS SOCIAUX ÉLECTRONIQUES

13.1 Le CSCDGR met en place des mesures afin de restreindre l'accès aux médias sociaux au sein des écoles pour les élèves.

13.2 Le CSCDGR reconnaît l'utilisation des médias sociaux électroniques comme un moyen viable de faire participer leurs collègues dans le dialogue scolaire, professionnel et promotionnel. Par conséquent, le CSCDGR s'engage à soutenir l'usage de médias sociaux électroniques sur les outils offerts par le Conseil pour les membres du personnel et les élèves afin qu'ils puissent interagir de façon informée et appropriée.

13.3 Le CSCDGR reconnaît que le personnel enseignant et les autres membres du personnel sont des modèles pour les élèves. Les parents, tuteurs ou tutrices partagent avec le personnel de l'école le devoir d'éduquer leurs enfants. Ainsi, le CSCDGR reconnaît que l'utilisation inacceptable des médias sociaux électroniques et d'Internet peut nuire au climat scolaire.

13.4 Toute utilisation de médias sociaux électroniques à des fins éducatives doit être exécutée de façon appropriée et responsable. Ainsi le discernement et l'utilisation éthique et responsable sont des composantes essentielles pour bénéficier des technologies disponibles, pour s'outiller et pour faciliter le réseautage entre professionnels.

13.5 Le CSCDGR reconnaît que les utilisateurs n'auront pas accès aux médias sociaux sur le réseau destiné aux invités.

14. SERVICES INFONUAGIQUES

14.1 Le CSCDGR reconnaît qu'il est avantageux d'avoir recours aux divers services infonuagiques. En plus d'être faciles à utiliser, les environnements infonuagiques permettent, entre autres :

- D'accéder à des technologies de pointe à des coûts abordables;
- d'augmenter ou de diminuer l'espace de stockage selon les besoins (extensibilité);
- d'accéder à distance aux données et aux logiciels en ligne;

- de faciliter le partage des informations et la collaboration entre les utilisateurs;
- de stocker et partager des documents, des photos, de la musique, des vidéos, etc.;
- d'utiliser des logiciels tels le traitement de texte et le tableur.

14.2 L'utilisation appropriée des environnements infonuagiques permet au personnel de partager et de cocréer efficacement et facilement un travail de groupe et, selon le cas, de développer les compétences des élèves dans leur utilisation des TIC au profit de leur apprentissage et des travaux réalisés en équipe.

14.3 L'utilisation des environnements infonuagiques aux fins de travail doit être autorisée par la personne responsable du Service informatique. Celle-ci vérifiera les politiques ou directives du fournisseur en ce qui a trait à la sécurité, à la vie privée ainsi qu'à toute autre exigence de gestion des technologies de l'information et des communications. Tout hébergement infonuagique d'information du CSCDGR, quelle qu'en soit la forme, sans autorisation préalable du CSCDGR est strictement interdit.

15. PHOTOS, EXTRAITS SONORES, TRAVAUX OU VIDÉOS

15.1 En tout temps, il est interdit de photographier, filmer ou enregistrer un extrait sonore à l'insu de la ou des personnes concernées.

15.2 Avant d'afficher les photos/extraits sonores/travaux ou vidéos, le personnel du CSCDGR doit s'assurer d'abord de protéger la confidentialité des renseignements personnels puis de s'assurer que l'affichage soit cohérent avec les objectifs pédagogiques du CSCDGR.

15.3 Si l'élève peut être identifié, le consentement écrit du parent, de la tutrice, du tuteur d'un élève de moins de 18 ans, d'un élève de 16 ans qui s'est soustrait de l'autorité parentale ou d'un élève de 18 ans et plus est requis pour tout affichage sur les médias sociaux.

15.4 L'affichage des photos, extraits sonores, travaux et des vidéos des élèves aux fins de développement professionnel ou d'apprentissage et dont le consentement écrit est signé, seront identifiés par le prénom de l'élève et le nom de l'école seulement.

15.5 Lors d'un événement public du CSCDGR, les personnes présentes sont autorisées à photographier, filmer ou enregistrer à la condition de respecter les pratiques du CSCDGR et les règlements de l'école. Toutefois le CSCDGR n'est pas en mesure de contrôler ni d'empêcher l'affichage, la distribution et l'utilisation de photos, de vidéos, d'images ou d'autres informations personnelles.

16. MESURES DISCIPLINAIRES OU ADMINISTRATIVES

16.1 Tout usage qui enfreint la présente directive administrative, y compris les lois et les règlements auxquels elle fait référence, les politiques et directives administratives du CSCDGR, ainsi que les règlements de l'école et de la salle de classe, risque selon la gravité de la situation, de mener notamment :

- À la suspension ou à la révocation du privilège d'accès à son appareil numérique personnel ou aux TIC du CSCDGR et de l'école, avec ou sans préavis;
- à un remboursement au CSCDGR pour les dommages ou les réparations subis à la suite du non-respect de la présente directive administrative;
- dans le cas d'une ou d'un élève, à une imposition de sanctions prévues en vertu de la politique administrative 6114 – Suspension d'un élève et 6115 – Renvoi d'un élève (en révision);
- dans le cas d'un membre du personnel, à des mesures disciplinaires selon les modalités prévues en vertu de la politique RH-08 : Mesures disciplinaires;
- dans le cas d'un consultant, aux sanctions prescrites dans l'entente de service;
- à une poursuite judiciaire par les autorités compétentes;
- à toute autre mesure administrative ou légale jugée appropriée.

16.2 Advenant que le CSCDGR prenne connaissance qu'un usager des TIC fait preuve d'une conduite criminelle, le CSCDGR peut également en informer les services policiers. D'autres circonstances peuvent aussi mener à la divulgation de renseignements obtenus à partir des TIC à d'autres autorités, notamment le Service à la famille et à l'enfance du Nord-Est de l'Ontario (SFENEO), l'Ordre des enseignantes et enseignants de l'Ontario, les autorités gouvernementales et tout autre organisme de réglementation professionnelle.

17. ENTENTE D'UTILISATION RESPONSABLE

17.1 Tout usager des technologies de l'information du CSCDGR doit lire et signer l'entente d'utilisation responsable des TIC qui précise les responsabilités liées à son utilisation, ainsi que les conséquences à la suite d'une infraction à la présente directive administrative.

17.2 L'accès aux TIC sera autorisé lorsque :

- Le membre du personnel aura remis à sa superviseure, son superviseur immédiat, le formulaire TIC01-01 - *Entente d'utilisation responsable des TIC* dûment signé; ce formulaire sera déposé au dossier du membre du personnel.
- Toute personne autorisée par le CSCDGR recevra l'information, soit le nom d'utilisateur et le mot de passe, du secteur des Services informatiques du CSCDGR. En accédant aux TIC, la personne confirme accepter de se conformer à la présente directive administrative.

18. RESPONSABILITÉS

18.1 Direction d'école :

18.1.1 Les directions d'école font part de toutes les nouvelles directives administratives ou procédés émis par la direction de l'éducation et secrétaire-trésorier à l'ensemble des membres du personnel de l'école, afin que ces directives et procédés soient mis en œuvre. Ces directives sont disponibles sur le site Web et lntranet du CSCDGR.

18.1.2 La direction d'école veille, en consultation avec le conseil d'école, à mettre en place le Code de conduite du CSCDGR et le Code de vie de l'école, conformément à la directive administrative portant sur l'utilisation des appareils personnels et l'accès aux médias sociaux (TIC-02).

18.1.3 La direction d'école met en œuvre un plan de citoyenneté numérique conforme au modèle fourni par le CSCDGR, tout en respectant les particularités de sa communauté scolaire. Ce plan doit faire partie intégrante du code de conduite de l'école. Le plan de citoyenneté permet aux écoles :

- D'identifier et d'appliquer les normes pour un comportement et une utilisation responsable de la technologie;
- d'encourager les élèves et le personnel à participer activement de façon éthique et sécuritaire aux activités en ligne;
- de guider les élèves et le personnel vers des comportements et une utilisation responsables des réseaux, des ressources numériques et de la technologie selon les processus identifiés dans la présente directive administrative.

18.1.4 La direction doit informer, au début de l'année scolaire, les élèves et leurs parents, tuteurs et tutrices du contrat d'engagement *Entente régissant l'utilisation responsable par les élèves des technologies de l'information et des communications* (TIC) et mettre à jour le plan de citoyenneté numérique de l'école au moins une fois par année pour répondre aux besoins émergents. Le plan révisé doit être dûment affiché.

18.2 <u>Membres du personnel, élèves, bénévoles et visiteurs</u> :

18.2.1 Le personnel enseignant doit consulter la *Recommandation professionnelle sur* l'utilisation *des moyens de communication électronique et des médias sociaux* affichée sur le site de l'Ordre des enseignantes et des enseignants de l'Ontario ainsi que la présente directive administrative.

18.2.3 Les membres du personnel, les élèves, les bénévoles et les personnes invitées ont la responsabilité de s'informer des attentes du CSCDGR quant à l'utilisation des TIC et de veiller au respect de l'ensemble des modalités de la présente directive administrative.

RÉFÉRENCES ET FONDEMENTS LÉGISLATIFS

- *Loi sur l'éducation – PPN 128*
- *Code des droits de la personne de l'Ontario*
- *Loi sur les droits d'auteur*
- *Code criminel du Canada*
- *Loi sur l'accès à l'information municipale et la protection de la vie privée*

DIRECTIVES ADMINISTRATIVES ASSOCIÉES

- Politique administrative 6108 – Discipline progressive (en révision)
- Politique administrative 6114 – Suspension d'un élève (en révision)

- Politique administrative 6115 – Renvoi d'un élève (en révision)
- Politique administrative 6116 – Code de conduite du CSCDGR (en révision)
- Politique administrative 8102 – Environnement sans fumée (en révision)
- RH-01 : Surveillance électronique des membres du personnel
- RH-03 : Déconnexion au travail
- RH-04 : Télétravail
- RH-08 : Mesures disciplinaires
- RH-13 : Perfectionnement professionnel (en révision)
- TIC-02 : Utilisation des appareils numériques personnels et accès aux médias sociaux– *en élaboration*

ANNEXES

Annexe 1 – Principes de citoyenneté numérique

Annexe 2 - La nétiquette

FORMULAIRES

TIC01-00 - Entente d'utilisation responsable des TIC (élèves) (en révision)

TIC01-01 - Entente d'utilisation responsable des TIC (membres du personnel) (en révision)

TIC-01 : Utilisation responsable des technologies de l'information et des communications	**ANNEXE 1 – Principe de citoyenneté numérique :**

La citoyenneté numérique englobe tous les aspects de la vie en ligne. Le citoyen de l'ère numérique a recours aux technologies de l'information et des communications (TIC) pour s'informer, se forger une opinion, échanger avec ses concitoyennes et concitoyens et s'exprimer dans un espace public.

Afin que la citoyenne, le citoyen de l'ère du numérique puisse participer activement et de façon positive à la vie en ligne, il doit comprendre et utiliser intelligemment les TIC. Elle ou il doit également développer les compétences qui lui permettront de discerner les risques et de veiller à la sécurité de soi et des autres.

Responsabilités de la citoyenne ou du citoyen (toute personne qui utilise les TIC.) à l'ère du numérique :

1. Agir avec respect, civisme et de manière éthique dans l'utilisation des TIC.
2. Utiliser la technologie de manière positive et significative.
3. Pratiquer l'utilisation sécurisée, légale et responsable des TIC.
4. Maintenir un climat positif, inclusif et tolérant pour tous, qui soutient la collaboration, l'apprentissage et la productivité quant à l'utilisation de la technologie.
5. Éviter de publier ou de divulguer des informations personnelles (nom, âge, adresse, numéro de téléphone, etc.) au sujet de soi et au sujet des autres.
6. Se familiariser avec la protection en ligne.
7. Assurer sa sécurité et gérer les risques.
8. Connaître ses droits et ses responsabilités.
9. Saisir les grands enjeux liés à la technologie.
10. Être sensibilisé ou sensibilisée au respect et à la protection de la vie privée en tenant compte de l'étendue des renseignements que nous transmettons et auxquels nous accédons grâce aux réseaux électroniques.
11. Respecter les valeurs du Conseil à titre d'institution catholique francophone.

TIC-01 : Utilisation responsable des technologies de l'information et des communications	ANNEXE 2 – Néthique et nétiquette

DÉFINITION

La néthique se définit comme étant des règles de conduite à caractère moral, les règles de politesse et de savoir-vivre que doivent emprunter les utilisateurs des TIC. Les actes illégaux posés lors de l'utilisation des TIC qui contreviennent à l'éthique sont, par exemple et sans s'y limiter, le piratage, la violation de données, l'atteinte aux droits d'auteur, la diffusion de documents illicites, toute atteinte au droit de la vie privée, entre autres à caractère pornographique ou à la propagande haineuse. Ces situations peuvent être considérées comme de la criminalité informatique.

RÈGLES DE LA NÉTHIQUE

1. Adoptez les mêmes règles de conduite en ligne que celles appliquées au quotidien.
2. Utilisez votre ordinateur dans une intention positive.
3. Collaborez positivement aux travaux des autres utilisateurs.
4. Respectez les fichiers et la propriété intellectuelle des autres utilisateurs.
5. Demandez la permission ou payez pour les logiciels personnels que vous désirez utiliser.
6. Pensez aux conséquences sociales des commentaires que vous écrivez et des discussions que vous entamez sur Internet.

LA NÉTIQUETTE

La nétiquette est la combinaison des mots *net* et *étiquette* et comprend les règles de politesse et de savoir-vivre que doivent emprunter les utilisateurs des TIC. Le pollupostage et la bombarderie sont des contre-exemples aux règles de courtoisie.

Règles de la nétiquette

1. **Faites preuve de clarté.** Il est approprié de remplir le champ « Objet » en indiquant clairement le sujet du message.

2. **Adaptez les formules de politesse dans vos courriers électroniques.** L'emploi de formules de politesse adaptées à l'interlocuteur est de mise (ex. : « Madame », « Monsieur » ou un simple « Bonjour » au début du courrier électronique et une formule de remerciement à la fin de la correspondance, telle « Merci pour votre aide ».
3. **Identifiez-vous et laissez vos coordonnées à la fin du message.** La signature devrait apparaître à la fin du message. Il est également approprié de laisser ses coordonnées, sans trop prendre de place.
4. **Soyez bref ou brève**. « Concis » et « précis » sont les qualificatifs à garder à l'esprit au cours de la rédaction d'un message dans Internet, que ce soit dans un courrier électronique, un commentaire dans un blogue ou au cours d'un échange dans un forum.
5. **Utilisez les majuscules avec discernement pour vous exprimer sur Internet**. L'emploi des majuscules peut correspondre à un cri sur Internet, que ce soit un message dans un courrier électronique, un commentaire sur une page Web ou un message dans un forum.
6. **Prenez le temps de vous relire**. Il est essentiel de vérifier le contenu du message envoyé. Cette pratique permet de revoir la structure des phrases, de corriger les fautes et de vous assurer que le langage utilisé est convenable. Cela s'avère particulièrement important lorsqu'un message est écrit sous l'effet de l'émotion ou au cours d'un échange conflictuel. Dans cette circonstance, il est préférable de se donner un peu de temps de réflexion avant de répondre au message.
7. **Respectez la vie privée des autres.** Il est important de connaître les règles en matière de déconnexion au travail (RH-03) et de respecter les horaires de travail lors d'envoi de courriel ou autres.
8. **Évitez le pollupostage**. L'envoi de courriels en chaîne ou de publicité à une personne ou à un groupe de personnes doit être évité.
9. **Ne répondez qu'aux personnes concernées**. Le bouton « Répondre à tous » devrait être utilisé avec discernement. Il faut éviter d'envoyer un message à un groupe de destinataires si ce n'est pas nécessaire.