Conseil scolaire du NORD-OUEST
4 Rue Bouchard, CP 1220 | St-Isidore (AB) | T0H 3B0
780.624.8855
www.csno.ab.ca

DIRECTIVE ADMINISTRATIVE 145

INFORMATION SÉCURISÉE

PRÉAMBULE

Le Conseil appuie l'utilisation d'environnements numériques et de services et les applications basées sur l'Internet (Cloud), ainsi que les services de stockage dans le nuage (Cloud) et de transfert de fichiers électroniques dans le but d'accomplir sa mission et ses activités.
Le Conseil reconnait que l'information, sous toutes ses formes, est essentielle à ses opérations courantes et qu'à ce titre, elle doit faire l'objet d'une saine gestion, d'une utilisation appropriée et d'une protection adéquate, le tout en conformité avec les différentes lois applicables.

Tout le personnel a une responsabilité légale et éthique lors de l'utilisation des actifs informationnels du Conseil. En vertu de la loi sur l'accès à l'information et de la protection de la vie privée (Freedom of Information and Protection of Privacy Act - FOIP) de l'Alberta, toutes les informations personnelles sont sensibles; par conséquent, la confidentialité doit être protégée pendant la collecte, le stockage, l'utilisation, le partage et la transmission de toutes les informations personnellement identifiables.. Le Conseil s'attend à ce que chaque utilisatrice et utilisateur des actifs informationnels se conforme aux dispositions de la Freedom of Information and Protection of Privacy Act de l'Alberta, de la Education Act, des lois et règlements, de la politique du conseil et des procédures administratives du Conseil.

OBJECTIF

La présente directive administrative encadre l'utilisation et la gestion des actifs informationnels du Conseil. Elle vise à établir les règles et les conditions applicables qui doivent être connues par toute personne ayant accès aux actifs informationnels du conseil, incluant l'accès aux informations d'un fournisseur ou d'un partenaire.
Cette présente directive administrative poursuit les objectifs suivants :

- Favoriser un usage efficace, respectueux, légal et sécuritaire de l'information et des technologies de l'information;
- Assurer une utilisation appropriée des applications basées sur l'internet (Cloud) ainsi que les services de stockage dans le nuage (Cloud) et le transfert de fichier électronique;

- Limiter les impacts des incidents de sécurité de l'information;
- Définir les droits et obligations des utilisateurs dans le respect des lois et règlements.

CHAMPS D'APPLICATION

La présente directive administrative s'applique à toute personne ayant accès aux actifs informationnels du Conseil, et ce, quels que soient son rôle et son lieu, est tenu de la connaître et de s'y conformer. Cette responsabilité s'étend à tout fournisseur ou partenaire du Conseil, incluant les sous-traitants.

DÉFINITIONS

Ces définitions sont présentées pour améliorer la compréhension de cette directive administrative :

Les applications basées sur le cloud sont des applications hébergées en dehors des installations du réseau interne de la Division.

Les installations de stockage de données basées sur le cloud sont des services de stockage de données qui fournissent un stockage de données sur des serveurs situés à l'extérieur des installations de réseau interne du Conseil scolaire.

Actif informationnel : une information, quel que soit son canal de communication (courriel, téléphone, etc.) ou son support papier ou électronique (serveur disque dur interne ou externe, etc.) un système ou une technologie de l'information ou un ensemble de ces éléments.

La citoyenneté numérique est définie comme le comportement généralement accepté de citoyenneté responsable qui est appliqué aux environnements en ligne et qui peut être considéré comme comprenant, mais sans s'y limiter, les éléments suivant :

- Traiter les autres avec dignité et respect ;
- Respecter la vie privée d'autrui ;
- Respecter les autres en s'abstenant de partager des informations les concernant à leur insu ou sans leur consentement ;
- Respecter les autres en s'abstenant d'utiliser un langage grossier ou abusif ;
- Respecter les autres en s'abstenant de publier ou de stocker tout contenu contenant des injures sexuelles, raciales, religieuses ou ethniques, toute autre forme d'abus, ou contenant un langage ou des images menaçants ou offensants ;
- Protéger vos informations personnelles contre des environnements, des agences ou des individus en ligne inconnus ou non compris ;

- N'effectuer des transactions financières en ligne qu'avec des agences connues, et seulement ensuite via des moyens sécurisés ;
- Respecter les autres en s'abstenant de toute action malveillante ou nuisible à leur égard;
- Respect du droit d'auteur ;
- Respecter et se conformer à la loi canadienne, qu'elle soit fédérale, provinciale, municipale ou autre;
- Respecter les lois ou les règles de tout autre agence internationale ou organisation avec laquelle vous interagissez ;
- S'assurer que vous êtes autorisé à accéder aux ressources à l'intérieur ou à l'extérieur du réseau du Conseil avant d'y accéder ;
- S'abstenir d'envoyer des fichiers ou des messages conçus pour perturber d'autres systèmes informatiques ou réseaux.

Un périphérique de stockage portable est considéré comme tout appareil mobile capable de stocker, de traiter ou de transmettre des informations numériquement. Cela comprend, mais sans s'y limiter : ordinateurs portables, tablettes, smartphones, clés USB/portables, CD/DVD.

Les informations personnelles en vertu de la loi FOIP désignent les informations enregistrées sur une personne identifiable, notamment :

- Nom, adresse personnelle ou professionnelle, ou numéro de téléphone personnel ou professionnel;
- Race, origine nationale ou ethnique, couleur ou croyances ou associations religieuses ou politiques;
- Âge, sexe, état matrimonial ou état de famille;
- Un numéro d'identification, un symbole ou tout autre particulier attribué à l'individu;
- Empreintes digitales, autres informations biométriques, groupe sanguin, informations génétiques ou caractéristiques héréditaires et ressemblance avec une photo;
- Des informations sur la santé et les antécédents médicaux de la personne, y compris des informations sur un handicap d'apprentissage, physique ou mental;
- Des informations sur les antécédents scolaires, financiers, d'emploi ou criminels de la personne, y compris les casiers judiciaires lorsqu'un pardon a été accordé;
- L'opinion d'un autre sur l'individu; et
- Les points de vue personnels ou opinions personnelles de la personne, sauf s'ils concernent quelqu'un d'autre.

Utilisatrice ou utilisateur : toute personne qui, dans le cadre de ses fonctions ou de ses études utilise l'information que le conseil détient dans l'accomplissement de sa mission, ou toute personne autorisée à accéder à une information appartenant au Conseil ou sous la responsabilité du Conseil. Les membres du personnel et les élèves sont les premiers utilisatrices et utilisateurs de l'information du Conseil.

DIRECTIVES GÉNÉRALES

1. Tous les renseignements personnels recueillis par le Conseil seront conservés et protégés contre tout accès non autorisé.
2. Les dispositifs de stockage portables ne doivent pas être utilisés pour stocker des renseignements personnels à moins d'y être autorisés par la direction générale. Les informations doivent être cryptées et protégées par mot de passe. Les informations personnelles sur les appareils portables doivent être temporaires et supprimées à la fin de la tâche.
3. L'administrateur du système d'information doit s'assurer que la sauvegarde et la récupération des données/informations sont en place et examinées périodiquement, concernant les informations stockées dans le réseau du Conseil.
4. Seules les personnes dument autorisées ont accès aux actifs informationnels du Conseil selon leurs fonctions et la nécessité de connaitre l'information qu'ils renferment. Le Conseil a le droit d'aviser la personne concernée que son usage des actifs informationnels n'est pas conforme et voir à ce que l'utilisation soit corrigée.
5. Chaque utilisatrice ou utilisateur est responsable des activités effectuées avec son compte d'utilisateur.
6. Le personnel du Conseil doit signaler toute atteinte à la sécurité des informations, à la confidentialité ou à l'abus des services cloud, qu'ils soient réels ou suspectés, à leur superviseur immédiat pour enquête. Les superviseurs doivent contacter l'administrateur du système d'information pour obtenir de l'aide.
7. Pour les applications ou le stockage basés sur le cloud pour lesquels un accord est conclu par l'enseignant, l'évaluation des risques liés à l'application et au stockage dans le cloud (formulaire A) sera complétée par l'enseignant et soumise à la direction.
8. Pour les applications ou le stockage basés sur le cloud pour lesquels un accord est conclu par l'école, l'évaluation des risques liés à l'application et au stockage dans le cloud (formulaire A) sera remplie par le directeur et soumise à l'administrateur des systèmes d'information.

9. Pour les applications ou le stockage basés sur le cloud pour lesquels un accord est conclu par le Conseil, l'évaluation des risques liés aux applications et au stockage en nuage (formulaire A) sera complétée par l'administrateur du système d'information.
10. Lorsqu'une violation ou un acte d'abus se produit, aucune mesure ne devrait être prise par l'enseignant ou l'école qui pourrait entraver une enquête jusqu'à ce que la direction générale l'ordonne.
    a. Aucune donnée ou information de compte ne doit être supprimée tant que la direction générale en fait la demande ou l'approuve.
    b. Les parents, les élèves ou les autres membres du personnel ne doivent pas être informés de la violation ou de l'abus avant d'y être dirigés par la direction générale.
11. L'utilisation d'applications ou de stockage basés sur le cloud par le personnel doit respecter les principes de « citoyenneté numérique ». De plus, le personnel est tenu de respecter ce qui suit lorsqu'il est en ligne :
    a. Pour les professionnels, le code de conduite propre à leur profession;
    b. Pour le personnel de soutien, les mêmes principes de conduite qui seraient attendus hors ligne;
    c. Pour tout le personnel, assurez-vous de ne pas publier ou partager d'informations liées au travail qui seraient considérées comme confidentielles; et
    d. Pour tout le personnel, comprenez que vos actions à la fois en ligne et hors ligne en dehors du travail peuvent affecter votre relation de travail avec le Conseil.
12. . Tout utilisateur ayant accès aux actifs informationnels du Conseil doit s'engager en signant le formulaire « Engagement à la confidentialité et à la protection des actifs informationnels » voir annexe A
13. Le Conseil veille également à ce que le personnel soit formé sur les procédures de sécurité du système informatique et sur l'utilisation correcte des actifs informationnels afin de minimiser les incidents.
14. Les atteintes à la vie privée doivent être signalées au coordonnateur FOIP.
15. L'utilisation de la visioconférence est restreinte à des fins d'enseignement, d'étude, de recherche ainsi qu'à des fins administratives, syndicales ou professionnelles. Tout enregistrement audio ou vidéo doit faire l'objet d'un consentement préalable de la part des participants.

Référence: Article 11, 31, 33, 52, 53, 196, 197, 222 Education Act
Freedom of Information and Protection of Privacy Act Canadian Charter of Rights and Freedoms
Canadian Criminal Code

La Charte canadienne des droits et libertés (art. 7)
Copyright Act
I.T.I.L. Standards, Alberta Education
ATA Code of Professional Conduct