DIRECTIVE ADMINISTRATIVE 145

INFORMATION SÉCURISÉE

Préambule

Le Conseil scolaire Centre-Est encourage l'utilisation d'environnements numériques et infonuagiques, les services de stockage dans le nuage (Cloud) ainsi que le transfert de fichiers électroniques dans le but d'accomplir sa mission et ses activités. Le CSCE reconnait que l'information, sous toutes ses formes, est essentielle à ses opérations quotidiennes 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.

L'ensemble du personnel du CSCE a une responsabilité légale et éthique face à l'utilisation des actifs informationnels du CSCE. En vertu de la Loi sur la protection de la vie privée *(Protection of Privacy Act - POPA)* et Loi sur l'accès à l'information (*Access to Information Act — ATIA*) 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 utilisateur des actifs informationnels se conforme aux dispositions de la loi ATIA et la loi POPA, de la Education Act, des lois et règlements appropriés et des directives administratives du CSCE.

Définitions

Les applications infonuagiques (basées sur le Cloud) sont des applications hébergées à l'extérieur des installations du réseau interne du CSCE.

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 du réseau interne du CSCE.

Actif informationnel : une information, quel que soit son canal de communication (courriel, téléphone, appareil électronique), son support (papier, électronique) ou le système dans lequel il se retrouve.

La citoyenneté numérique est définie comme le comportement généralement adopté par un citoyen responsable qui est appliqué aux environnements en ligne et qui peut comprendre, sans s'y limiter, les éléments suivants:

- Traiter les autres avec dignité et respect;
- Respecter la vie privée des autres;
- Respecter les autres en s'abstenant de
  - Partager des informations les concernant à leur insu ou sans leur consentement;
  - D'utiliser un langage grossier ou abusif;
  - Publier ou de stocker tout contenu contenant des injures à caractère sexuel, raciale, religieux ou ethnique ou toutes autres formes d'abus, ou contenant un langage ou des images menaçants ou offensants;
  - Toutes actions malveillantes ou nuisibles à leur égard;
- Protéger ses informations personnelles contre des environnements, des agences ou des individus en ligne inconnus;

- N’effectuer des transactions financières en ligne qu’avec des agences connues et uniquement via des moyens sécurisés;
- Respecter les droits d’auteur;
- Respecter les lois ou les règles de la loi canadienne, qu’elle soit fédérale, provinciale, municipale ou autre.

Un périphérique de stockage portable est considéré comme tout appareil mobile capable de stocker, de traiter ou de transmettre des informations numériques. Cela comprend, sans s’y limiter, des ordinateurs portables, tablettes, téléphones intelligents, clés USB, CD.

Les informations personnelles en vertu de ATIA et POPA désignent les informations identifiables enregistrées sur une personne, notamment

- Nom, adresse personnel ou professionnelle, ou numéro de téléphone personnel ou professionnelle, adresse électronique personnel ou professionnelle, ou d'autres coordonnées, sauf lorsque la personne a fourni ces informations au nom de son employeur ou mandant, dans le cadre de ses fonctions à titre d’employé ou de mandataire.
- Race, origine nationale ou ethnique, couleur ou croyances ou associations religieuses ou politiques;
- Âge, sexe, identité de genre, orientation sexuelle état matrimonial ou état familial;
- Un numéro d’identification, un symbole ou toute autre particularité attribuée à l’individu;
- Empreintes digitales, autres informations biométriques, groupe sanguin, informations génétiques ou caractéristiques héréditaires;
- Informations sur la santé et les antécédents médicaux de la personne, y compris des informations sur sa santé physique ou mental;
- 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 de la personne, sauf s’ils concernent une autre personne.

Utilisateur: toute personne qui, dans le cadre de ses fonctions ou de ses études utilise l’information que le conseil détient dans la réalisation de ses fonctions, 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 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, pour le réseau interne du Conseil, les mesures pour la sauvegarde et la récupération des données/informations sont en place et que celles-ci sont examinées.

4. Seules les personnes dument autorisées ont accès aux actifs informationnels du Conseil selon leurs fonctions. Le Conseil se réserve le droit d’aviser l’individu concerné que son utilisation des actifs

informationnels n'est pas conforme aux attentes et doit voir à ce que l'utilisation soit corrigée.

5. Chaque 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 pour obtenir de l'appui.

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 doit être complété par l'enseignant et remis à la direction de l'école.

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 doit être complété par la direction de l'école et remis à l'administrateur des systèmes.

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 à l'application et au stockage dans le Cloud doit être complété par l'administrateur du système.

10. Lorsqu'il y a violation ou abus, aucune mesure ne devrait être prise par l'enseignant ou l'école qui pourrait nuire à une enquête jusqu'à ce que la direction générale l'autorise.

11. L'utilisation d'applications ou de stockage basée sur le Cloud par le personnel doit respecter les principes de citoyenneté numérique, des énoncés de la DA 141 et du code de conduite du CSCE.

12. Plus spécifiquement, pour Google en éducation, il est entendu que le personnel et les élèves du CSCE auront accès à la suite Google en éducation.

- Les travaux créés dans cette suite par l'utilisateur sont enregistrés sur les serveurs de Google.
- Un compte Google est créé, par le CSCE, pour le personnel et les élèves afin qu'ils puissent accéder à la suite. Ce compte est pour des fins professionnels et scolaire et doit être utilisé uniquement dans l'exercice de ses fonctions respectives.
- Lorsque l'utilisateur stock des documents dans la suite Google, il est important d'utiliser les mesures de sécurité prévues et de bien contrôler l'accès à ces documents.
- Aucune information confidentielle ne doit figurer dans un document Google ou dans les documents téléversés dans Google Drive.
- À la fin d'un contrat de travail, tous les accès à Google pour éducation sont automatiquement supprimés. Les données des finissants et des élèves transférés vers d'autres établissements scolaires seront supprimées après une période de deux mois.

Références:
Articles 11, 31, 33, 52, 53, 196, 197, 222 Education Act
Loi sur l'accès à l'information (ATIA)
Loi sur la protection de la vie privée (POPA)
Charte des droits et libertés (Article 7)
Copyright Act
Canadian Criminal Code

Adopté le 28 août 2025