

Conseil scolaire
francophone provincial

POLITIQUE

Section : Technologies de l'information

Objet : Utilisation acceptable de la technologie

N° : TI-01

Adoption de CSFP : 25.11.2021

En vigueur: 25.11.2021

Dernière révision: 30.03.2025

Dans le but d'alléger le texte, les formes au masculin du présent document désignent aussi bien les femmes que les hommes à moins que le contexte n'en indique le contraire.

TITRE DE LA POLITIQUE

Utilisation acceptable de la technologie

Préambule

Le Conseil scolaire francophone provincial (CSFP) soutient l'utilisation des technologies de l'information et de la communication (TIC) dans les programmes d'instruction pour faciliter l'enseignement et l'apprentissage par le biais des communications interpersonnelles, de l'accès à l'information, de la recherche et de la collaboration, et pour appuyer les fonctions administratives du système scolaire public. Le CSFP s'engage à fournir un environnement technologique accessible, fiable et sécurisé pour le personnel, les élèves et les invités aux fins d'enseignement, d'apprentissage et d'utilisation administrative.

Le CSFP reconnaît que la protection de l'intégrité de tous les systèmes TIC et la sécurité, la confidentialité et la sûreté de tous les élèves et du personnel sont d'une importance capitale. Par conséquent, le conseil exige une utilisation acceptable, éthique, légale et responsable de tous les systèmes TIC.

Contexte

Le CSFP reconnaît la valeur et le besoin de la technologie dans le cadre éducatif et, par conséquent, offre au personnel et aux élèves du Conseil scolaire francophone provincial l'accès aux systèmes TIC, incluant l'accès à Internet. À cet effet, le Conseil scolaire francophone provincial investit des ressources importantes dans l'achat, le développement et l'utilisation des systèmes TIC pour le personnel enseignant et les élèves. Le personnel informatique du Conseil scolaire

francophone provincial fournira éducation et sensibilisation au personnel et aux élèves pour une utilisation responsable de la technologie.

L'intégration de la technologie dans les pratiques quotidiennes en classe améliore l'environnement d'apprentissage des élèves, en soutenant l'acquisition des compétences en littératie, numératie et apprentissage de haut niveau. Dans le cadre de sa mission et de sa vision, les systèmes TIC aident à préparer les élèves à réussir dans la vie et au travail au XXI^e siècle. Utilisés de manière appropriée, ces outils technologiques offrent des ressources d'information mondiales, des occasions de collaboration et de communication, ainsi que des expériences d'enseignement et d'apprentissage riches en médias pour les élèves et le personnel enseignant.

Champ d'application

Cette politique s'applique à tous les élèves, au personnel et aux utilisatrices et utilisateurs autorisés des systèmes TIC au sein du Conseil scolaire francophone provincial.

Définitions

Pour les besoins de la politique sur l'utilisation acceptable de la technologie :

TIC

Les TIC (Technologies de l'information et de la communication) désignent les outils et ressources technologiques utilisés pour communiquer, créer, distribuer, stocker et gérer l'information. Ces technologies incluent, mais ne se limitent pas à, tout le matériel informatique, les logiciels de systèmes d'exploitation, les logiciels applicatifs, les fichiers de texte et de données stockés. Cela comprend, mais sans s'y limiter, au courrier électronique, aux bases de données locales, aux bases de données accessibles à distance, aux ordinateurs de bureau/portables, aux supports magnétiques ou optiques enregistrés, aux cliparts, aux images numériques, aux informations numérisées, ainsi qu'aux technologies et appareils de communication, etc.

Internet

Réseau informatique mondial interconnectant d'autres réseaux informatiques, sur lequel sont situés des services pour utilisateurs finaux, tels que des sites Web ou des archives de données, permettant d'accéder aux données et de les échanger.

Utilisateur autorisé

Un utilisateur autorisé est un individu qui est approuvé et a reçu des permissions pour utiliser ou accéder à une ressource technologique particulière telle que des ordinateurs, des dispositifs informatiques, des bases de données, des courriers électroniques et d'autres ressources technologiques. Le niveau d'accès aux ressources technologiques et aux réseaux sera déterminé par fonction et besoin par le personnel désigné du système scolaire public par le personnel informatique du CSFP.

Surveillance des communications électroniques

La surveillance des communications électroniques fait référence à l'utilisation de mécanismes tels que les pare-feux, les filtres web, etc., pour accéder, examiner et analyser par la suite l'activité, les informations ou l'utilisation de tout système ou réseau TIC.

Directives

1. Chaque école doit intégrer la *Politique d'utilisation acceptable de la technologie* et les procédures administratives dans leurs pratiques scolaires.
2. Tous les utilisateurs autorisés doivent signer l'*Entente pour l'utilisation acceptable de la technologie*, définissant l'accès, les attentes d'utilisation et les sanctions en cas d'utilisation inappropriée.
3. Le ministère de l'Éducation et ses agents ont le droit, mais non l'obligation, de surveiller toute utilisation de la technologie pour garantir la conformité avec les attentes définies dans cette politique.
4. Le ministère conserve le droit d'accéder, d'inspecter, d'enquêter et de surveiller toute utilisation et ses ressources, y compris tous les fichiers de données, les réseaux de communication et les informations créées sur, avec ou transmises à l'aide de ses ressources TIC, y compris les courriels, les messages texte, l'utilisation d'Internet et toute autre communication ou information. Tous ces fichiers, communications ou informations peuvent être surveillés, examinés ou accessibles par le personnel autorisé à le faire et ayant une raison appropriée en vertu de questions civiles et pénales, à des fins d'enquête ou pour toute autre raison légale, y compris, mais sans s'y limiter aux cas suivants :
 - a) Il existe des motifs raisonnables de soupçonner des abus, une non-conformité avec les politiques/procédures, ou des activités inappropriées ou illégales.
 - b) Cela est requis par une citation à comparaître ou une ordonnance du tribunal.

c) Cela est nécessaire pour répondre à une demande d'accès à l'information ou à une violation présumée de la vie privée en vertu de la [Loi sur l'accès à l'information et la protection de la vie privée \(LAIPVP\)](#).

d) Cela est nécessaire pour effectuer un audit ou garantir la sécurité et la performance opérationnelle des ressources TIC.

La surveillance et les recherches, si nécessaire, seront effectuées par un ou une membre du personnel désigné par la surintendance des écoles.

5. Le ministère se réserve le droit de bloquer, de limiter ou d'interdire toute application, site web, adresse ou protocole jugé inacceptable ou qui impose une charge à l'infrastructure TIC.

6. Les utilisateurs de l'infrastructure TIC du Conseil scolaire francophone provincial sont tenus de se comporter comme ils le feraient dans tout autre environnement où ils représentent leur école. Les utilisateurs doivent se conduire de manière responsable, éthique et respectueuse.

7. Les systèmes TIC sont fournis pour améliorer la prestation des programmes éducatifs et des services de soutien connexes ainsi que pour mener d'autres activités scolaires.

Procédures administratives

Généralités :

1.1. Les ressources technologiques sont destinées à des fins éducatives et à la gestion des opérations du CSFP.

1.2. L'utilisation des ressources technologiques doit soutenir la réussite des élèves et être cohérente avec la mission et les objectifs du CSFP et des écoles.

1.3. Les utilisateurs doivent suivre les mêmes règles de bonne conduite et de respect en ligne qu'ils respectent hors ligne.

1.4. Le CSFP prendra toutes les mesures raisonnables pour assurer la sécurité des utilisateurs en ligne, mais ne sera pas tenu responsable des dommages ou préjudices résultant de l'utilisation des ressources technologiques du CSFP.

1.5. Les utilisateurs doivent alerter l'administration scolaire, le superviseur ou le personnel des technologies de l'information du CSFP de toute préoccupation concernant l'utilisation abusive, la sécurité, la confidentialité ou la sûreté des ressources technologiques.

1.6. L'utilisation des ressources technologiques dans les écoles est soumise à toutes les politiques, règlements et pratiques du CSFP en matière de technologie, de propriété et de conduite.

1.7. Les utilisateurs ayant accès à des données personnelles ou confidentielles doivent utiliser toutes les précautions appropriées pour maintenir l'exactitude, l'intégrité et la confidentialité des données et s'assurer qu'aucune divulgation non autorisée ne se produise.

1.8. Une utilisation personnelle limitée des ressources technologiques est permise à condition que cette utilisation :

1.8.1. Ne viole cette politique ou une autre politique ou réglementation du CSFP ;

1.8.2. N'interfère pas avec la productivité du personnel ;

1.8.3. N'interfère avec les opérations du CSFP ;

1.8.4. N'interfère avec les opérations informatiques ;

1.8.5. Ne compromets pas le CSFP de quelques manières.

Utilisation des dispositifs personnels sur le réseau du CSFP

Si un utilisateur choisit d'apporter son appareil électronique/informatique personnel et de le connecter au réseau du Conseil scolaire francophone provincial, la *Politique d'utilisation acceptable de la technologie* reste applicable, ainsi que ce qui suit :

2.1. Les dispositifs personnels ne doivent pas être connectés au réseau du CSFP si des applications de partage de fichiers (Post-à-Post — P2P) tels que, mais sans se limiter à Limewire, BitTorrent, uTorrent, Shareaza, etc., sont présentes. Ces applications doivent être complètement supprimées du dispositif avant de se connecter au réseau d'une école ou du CSFP.

2.2. Les utilisateurs qui connectent leur dispositif personnel au réseau du CSFP doivent s'assurer que leur dispositif est protégé par un mot de passe.

2.3. Les utilisateurs sont responsables de la sécurité, de l'entretien et de la maintenance de leur propre dispositif.

2.4. Les utilisateurs doivent s'assurer que leur dispositif est protégé par une application antivirus/antimaliciel d'entreprises telles que Symantec, Microsoft, McAfee, etc.

2.5. Les utilisateurs sont entièrement responsables de leur dispositif personnel lorsqu'il est à l'école. Le CSFP n'est pas responsable de la perte, du vol ou des dommages causés au dispositif.

2.6. Les dispositifs personnels (p. ex. iPads, téléphones cellulaires, ordinateurs portables appartenant aux élèves) sont autorisés dans les écoles, conformément aux lignes directrices cohérentes à l'échelle de l'école déterminées par l'administration et le personnel de l'école.

2.7. L'utilisation des dispositifs personnels en classe doit être à des fins éducatives uniquement, conformément aux lignes directrices et pratiques cohérentes à l'échelle de l'école déterminées par l'administration et le personnel de l'école.

2.8. Une utilisation inappropriée des dispositifs/technologies personnels entraînera des conséquences, comme indiqué dans l'*Entente pour l'utilisation acceptable de la technologie* —

Élèves et parents/tuteurs.

2.9. En général, l'utilisation des dispositifs personnels n'est pas autorisée dans les salles de classe de la maternelle à la 6e année, sauf dans des circonstances où leur utilisation est requise pour soutenir les besoins d'apprentissage documentés des élèves individuels. Cette détermination est faite par l'administration de l'école, en consultation avec le personnel approprié.

3. Sécurité

3.1. Les utilisateurs ne doivent pas télécharger ou tenter de télécharger ou d'exécuter des applications non autorisées sur le réseau de l'école sans l'autorisation expresse du personnel des technologies de l'information du CSFP.

3.2. Les utilisateurs ne doivent pas introduire, créer ou propager des programmes malveillants, y compris, sans limitation, des virus, des vers, des chevaux de Troie, des logiciels espions ou tout autre code malveillant, sur tout système du CSFP.

3.3. Si un utilisateur croit qu'un ordinateur est infecté par un virus ou un logiciel malveillant, il doit arrêter immédiatement d'utiliser le système et signaler l'incident à l'administration scolaire ou au personnel des technologies de l'information du CSFP.

3.4. Les utilisateurs ne doivent pas tenter de supprimer le virus ou le logiciel malveillant ou télécharger des programmes pour aider à les supprimer.

3.5. Les utilisateurs ne doivent pas falsifier des équipements matériels, des réseaux, des applications, des systèmes de réseau, des ordinateurs ou des fichiers d'autres utilisateurs sans autorisation ou permission. En particulier, les utilisateurs ne doivent pas :

- Tenter d'obtenir un accès non autorisé aux données du CSFP/école/autres ;
- Tenter de vandaliser les systèmes du CSFP ;
- Contourner ou altérer les logiciels, protections physiques ou autres restrictions technologiques placées sur les ordinateurs, réseaux, logiciels, applications ou fichiers, y compris les logiciels de protection antivirus installés par le gouvernement ;
- Lancer des attaques ou des sondes, ou tenter autrement de subvertir la sécurité de tout système ou réseau.

4. Accès à Internet

L'utilisation d'un navigateur web pour accéder à Internet peut potentiellement exposer les utilisateurs finaux à du matériel inacceptable et à d'autres contenus répréhensibles. Pour lutter contre cette exposition à de telles menaces, le Conseil scolaire francophone provincial filtre les sites web jugés inappropriés comme stratégie de sécurité pour protéger les utilisateurs en ligne.

4.1. Les utilisateurs sont tenus de considérer le filtre web comme une mesure de sécurité, et en aucun cas, les utilisateurs ne doivent essayer de le contourner lorsqu'ils naviguent sur Internet.

Aucun système de filtrage n'étant parfait, le Conseil scolaire francophone provincial ne peut pas garantir que tout le matériel inacceptable ou répréhensible sera complètement filtré.

5. Mots de passe

Les noms d'utilisateur et les mots de passe (identifiants d'accès) contribuent à garantir la sécurité et la confidentialité des données stockées sur divers systèmes et serveurs du système scolaire public. En tant qu'utilisateur, il est de votre responsabilité de vous assurer que tous vos mots de passe de compte soient aussi difficiles à deviner que possible.

5.1. Tous les mots de passe utilisés au sein du Conseil scolaire francophone provincial doivent répondre à des exigences strictes et avoir les caractéristiques suivantes :

5.2. Les mots de passe doivent respecter les exigences minimales suivantes :

- Être composés d'au moins huit caractères.
- Contenir des caractères de trois des quatre catégories suivantes :
 - Caractères majuscules anglais (A à Z)
 - Caractères minuscules anglais (a à z)
 - Chiffres de base 10 (0 à 9)
 - Caractères spéciaux (par exemple !, \$, #, %)

5.3. Ne jamais écrire votre mot de passe pour s'en souvenir.

5.4. Certains systèmes attribueront un mot de passe par défaut à un utilisateur pour accéder au système. Ce mot de passe doit être changé immédiatement lors de la première connexion de l'utilisateur.

5.5. Les utilisateurs sont responsables et redevables de toute activité effectuée dans leur(s) compte(s) protégé(s) par mot de passe.

5.6. Une fois le travail terminé, les utilisateurs doivent se déconnecter de chaque compte protégé par mot de passe.

5.7. Si vous soupçonnez une manipulation d'un mot de passe réseau, informez immédiatement l'administration de l'école, un superviseur ou contactez immédiatement le personnel des technologies de l'information du Conseil scolaire francophone provincial.

5.8. Les utilisateurs sont responsables de la sécurité et de la protection de tous les comptes protégés par mot de passe qui leur sont attribués (nom d'utilisateur et mot de passe).

5.9. En aucun cas, un utilisateur ne doit partager ses informations de connexion attribuées avec

un autre utilisateur ni se connecter en utilisant le nom d'utilisateur et le mot de passe d'un autre utilisateur.

6. Transport d'informations personnelles ou confidentielles

6.1. L'utilisation de CD, DVD ou clés USB non chiffrés pour transporter des informations confidentielles ou personnelles est interdite.

6.2. Le transport d'informations personnelles ou confidentielles doit se faire à l'aide d'un appareil chiffré (par exemple, clé USB chiffrée, volume chiffré sur un ordinateur portable).

6.3. Les utilisateurs doivent limiter la quantité d'informations personnelles ou confidentielles transportées ou emportées à domicile. Par exemple, ne prendre que le nom de l'élève et non d'autres informations permettant d'identifier l'élève.

6.4. Les utilisateurs doivent transporter des informations personnelles uniquement lorsque cela est nécessaire, et ne pas laisser les informations sur l'appareil par la suite.

7. Dispositifs réseau non autorisés

Les dispositifs réseau tels que les points d'accès sans fil, les commutateurs, les routeurs, les points d'accès Wi-Fi, etc., qui ne sont pas autorisés, installés et configurés par le personnel de la des technologies de l'information du Conseil scolaire francophone provincial, sont considérés comme des dispositifs clandestins et représentent un point d'entrée ouvert et non sécurisé dans notre réseau. Ces dispositifs clandestins peuvent contourner la sécurité du réseau et exposer le réseau à des menaces de sécurité.

7.1. L'extension d'un réseau du Conseil scolaire francophone provincial ou d'un réseau scolaire par l'introduction d'un dispositif clandestin tel qu'un point d'accès sans fil, un commutateur, un routeur, un point d'accès Wi-Fi, ou tout autre service ou dispositif est strictement interdite.

8. Utilisation inacceptable

8.1. Participer à tout acte illégal ou enfreindre toute loi locale, provinciale ou fédérale.

8.2. Dupliquer, stocker ou transmettre des documents pornographiques ou répréhensibles.

8.3. Utiliser le réseau du Conseil scolaire francophone provincial et/ou Internet à des fins illégales, criminelles, de jeux d'argent en ligne ou autres fins inappropriées, ou pour soutenir de telles activités.

8.4. Accéder, examiner, télécharger, stocker, imprimer, publier ou distribuer du matériel ou du contenu qui est criminel, illégal, incendiaire, discriminatoire (littérature haineuse), abusif, obscène, impoli, grossier, profane, sexuellement explicite, qui soutient la violence ou qui est harcelant/intimidant/menaçant.

8.5. Dupliquer, installer, stocker ou transmettre du matériel protégé par des droits d'auteur de manière illégale ou non autorisée.

8.6. Publier des informations fausses, insultantes ou attaquer personnellement une personne.

8.7. Se connecter à un système informatique en utilisant les informations de compte d'un autre utilisateur.

8.8. Utiliser des applications de partage de fichiers non autorisées ou télécharger ou partager des fichiers illégalement, y compris, sans limitation, des films, de la musique, des applications et d'autres logiciels.

8.9. Les applications Peer-2-Peer (poste à poste) telles que, mais sans s'y limiter, Limewire, BitTorrent, uTorrent, Shareaza, etc., sont strictement interdites.

8.10. Utiliser le réseau du Conseil scolaire francophone provincial à des fins commerciales, financières, politiques ou autres gains personnels connexes.

8.11. Installer des logiciels de tout type sur des ordinateurs sans l'autorisation directe du personnel des technologies de l'information du Conseil scolaire francophone provincial.

8.12. Partager ou publier des informations personnellement identifiables, y compris, mais sans s'y limiter : adresse, numéro de téléphone ou photo non autorisée.

8.13. Détruire, endommager ou désactiver tout équipement informatique (matériel ou logiciel).

8.14. Essayer d'accéder aux informations ou au compte de quelqu'un d'autre sans autorisation.

9. Violations

Les violations de ces règlements peuvent entraîner une restriction, une suspension ou une révocation de l'accès aux technologies du CSFP et peuvent entraîner des mesures disciplinaires.

Les violations de cette politique peuvent être signalées aux autorités judiciaires appropriées et peuvent également faire l'objet d'enquêtes ou de poursuites judiciaires. Les utilisateurs sont également informés que l'utilisation inappropriée pourrait entraîner :

1. Des poursuites pénales en vertu du Code criminel et d'autres lois canadiennes ou provinciales.
2. Des actions civiles le cas échéant (p. ex. dommages intentionnels au réseau informatique, matériel informatique, logiciels, etc.).

10. Déclaration de non-responsabilité

Les services technologiques et les systèmes d'information du CSFP sont fournis « en l'état », « selon la disponibilité ». Le CSFP n'offre aucune garantie ou assurance de quelque manière que ce soit, exprimé ou implicite au sujet de la fiabilité et la disponibilité de la technologie qu'il fournit et ne sera pas responsable des dommages qui pourraient résulter de l'utilisation de toute



technologie. Cela inclut la perte de données résultant de retards, de non-livraisons, de livraisons manquées ou d'interruptions de service causées par des erreurs technologiques ou des erreurs ou omissions d'utilisateurs. L'utilisation de toute information obtenue ou fournie via Internet ou par courriel est aux risques de l'utilisateur. Le CSFP décline toute responsabilité quant à l'exactitude ou la qualité des informations obtenues par le biais de ses services technologiques.

ANNEXE A

À lire par la famille avant de signer l'entente

1. Entente pour l'utilisation acceptable de la technologie pour les élèves et les parents/tuteurs

L'utilisation des appareils électroniques fait désormais partie de la vie quotidienne de la plupart des élèves. Ces appareils peuvent améliorer l'apprentissage et engager les élèves en classe. Notre école utilise des dispositifs électroniques tels que des ordinateurs, des tableaux blancs interactifs, des tablettes et d'autres appareils mobiles en classe pour améliorer les résultats scolaires et motiver les élèves. L'utilisation du réseau de l'école, l'accès aux ressources d'apprentissage et aux applications (apps) aident tous les élèves à atteindre leurs objectifs d'apprentissage.

Pour protéger tous les élèves, des lignes directrices et des pratiques d'utilisation appropriées pour ces appareils doivent être établies, suivies et surveillées.

Tous les parents/tuteurs doivent signer l'Entente pour l'utilisation acceptable de la technologie avant que les élèves ne soient autorisés à utiliser/accéder à la technologie et aux ressources en ligne à l'école. Cet entente a pour but de:

- S'assurer que les élèves et les parents/tuteurs sont conscients des conditions sous lesquelles les élèves sont autorisés à utiliser la technologie ;
- Définir les attentes et les responsabilités des élèves en matière d'utilisation appropriée et inappropriée de la technologie ;
- S'assurer que les élèves et les familles sont conscients de leurs responsabilités pour protéger la vie privée individuelle.

Nous demandons aux parents et tuteurs de surveiller l'utilisation et de discuter de ces attentes et responsabilités ainsi que de la bonne utilisation de la technologie avec leurs enfants, et nous vous remercions de votre soutien.

Services en ligne / “Services cloud”

Certains outils en ligne et applications sont appelés “services cloud”. Cela signifie que les élèves enregistreront leur travail en ligne. L'utilisation des services cloud ou des ressources en ligne permettra aux élèves de travailler sur des projets en dehors du temps scolaire. Les écoles fourniront à chaque élève un nom d'utilisateur, un mot de passe et une adresse e-mail.

La protection de la vie privée en ligne est une priorité absolue pour notre école et le ministère de l'Éducation, et nous protégeons le travail en ligne de nos élèves au mieux de nos capacités. Les familles et les élèves ont un rôle à jouer dans la protection de la vie privée des informations.

Écoles sécuritaires et bienveillantes

Tous les élèves sont tenus de respecter le code de conduite de l'école lorsqu'ils utilisent la technologie, accèdent à Internet et interagissent en ligne.

Accès à Internet et filtrage

Toutes les écoles fournissent désormais un accès à Internet pour l'enseignement et l'apprentissage. Internet contient une richesse de matériel éducatif pour la classe, mais peut également contenir du matériel inapproprié. Le Conseil scolaire francophone provincial filtre les sites web jugés inappropriés pour les élèves. Le Conseil scolaire francophone provincial ne peut garantir que tout le matériel inapproprié sera complètement filtré.

Courriel

Les élèves recevront un compte Gmail à des fins de courrier électronique, par exemple JDoe_s@csfp.ca. Toutes les adresses e-mail des élèves contiennent un trait de soulignement (_) et un « s ».

Pour plus d'informations, consultez la [Politique de courrier électronique du Conseil scolaire francophone provincial] (Conseil scolaire francophone provincial E-mail Policy).

Médias sociaux

Le Conseil scolaire francophone provincial reconnaît que les médias sociaux (par exemple, Facebook, Twitter, MySpace, etc.) sont des outils qui peuvent améliorer davantage l'enseignement et l'apprentissage dans nos écoles, ainsi que la communication entre la maison et l'école et avec le public. Les élèves peuvent avoir l'occasion d'accéder à diverses formes de médias sociaux à l'école. Des informations supplémentaires seront fournies au niveau de l'école.

Pour plus d'informations, consultez la *Politique de médias sociaux* du Conseil scolaire francophone provincial.

Appareils portables

L'utilisation des appareils électroniques portables (par exemple, iPads, iPhones, ordinateurs portables) fait désormais partie de la vie quotidienne de la plupart des élèves. Ces appareils favorisent l'engagement, la créativité et l'apprentissage des élèves. De nombreuses écoles disposent désormais de jeux d'appareils disponibles pour une utilisation en classe. Les élèves peuvent également être autorisés à utiliser leurs propres appareils électroniques portables à l'école, conformément aux directives cohérentes de l'école établies par l'administration et le personnel scolaire. Cette entente pour l'utilisation acceptable de la technologie s'applique, que l'élève utilise un appareil appartenant à l'école ou personnel.

Utilisation acceptable de la technologie

a. La technologie doit être utilisée pour des activités éducatives et d'apprentissage, ainsi que pour d'autres fins autorisées par l'administration de l'école.

b. L'utilisation des appareils personnels (par exemple, iPads, téléphones portables, ordinateurs portables appartenant aux élèves) pendant les heures de classe doit être réservée à des fins éducatives uniquement, conformément aux directives et pratiques cohérentes de l'école établies par l'administration et le personnel scolaire. Veuillez noter que les sorties scolaires sont considérées comme des heures de classe.

c. Les élèves doivent respecter toutes les politiques de la Direction des opérations éducatives et de l'école lorsqu'ils utilisent la technologie et traiter les autres avec respect en tout temps.

d. Les appareils électroniques portables sont autorisés dans les salles où se déroulent des examens, avec la permission de l'enseignant. Par exemple, une autorisation doit être obtenue pour utiliser un appareil comme calculatrice.

e. En général, l'utilisation des appareils personnels n'est pas autorisée dans les classes de la maternelle à la 6e année, sauf dans les cas où leur utilisation est nécessaire pour soutenir les besoins d'apprentissage documentés des élèves. La décision est prise par l'administration de l'école, en consultation avec le personnel approprié.

Les actions suivantes sont interdites :

- Tenter d'accéder aux informations ou au compte de quelqu'un d'autre sans permission ;
- Partager ou publier des informations personnellement identifiables (telles que des photos, numéros de téléphone et adresses) en ligne ;
- Rencontrer en personne quelqu'un rencontré en ligne sans la connaissance et la permission des parents ;
- Enfreindre les accords de licence ou de droits d'auteur ; copier les idées, le travail ou les écrits d'une autre personne ou source ; et
- Participer à des activités pouvant être considérées comme du harcèlement ou de l'intimidation des autres ou participer à des activités perturbant l'environnement scolaire.

Attentes

Les élèves utilisateurs doivent :

a. Se comporter comme ils le feraient dans tout autre environnement où ils représentent leur école et/ou le Conseil scolaire francophone provincial. Les élèves doivent se conduire de manière responsable, éthique et respectueuse conformément aux normes du Conseil scolaire francophone provincial.

- b. Obtenir la permission du directeur ou de son représentant pour prendre des photos ou faire des enregistrements dans l'environnement scolaire ou lors d'activités parrainées par l'école.
- c. S'abstenir de partager ou de publier des photos/enregistrements pris dans l'environnement scolaire ou lors d'activités parrainées par l'école, sans le consentement direct de chaque personne incluse.
- d. S'assurer que leur appareil mobile est chargé avant de venir à l'école - il peut y avoir un nombre limité de prises électriques disponibles.
- e. Prendre les mesures appropriées, comme éteindre les sonneries, pour que l'appareil mobile personnel ne perturbe pas le temps d'instruction.
- f. S'assurer que leur appareil est toujours rangé dans un endroit sûr et sécurisé.
- g. Garder les noms d'utilisateur et les mots de passe privés et respecter la vie privée des autres.
- h. Se déconnecter lorsqu'ils n'utilisent pas leur compte de messagerie.
- i. Utiliser toutes les technologies de manière responsable et ne pas abuser ou endommager délibérément l'équipement ou les réseaux.
- j. Être responsables de leurs propres appareils mobiles. L'école ou le gouvernement n'est pas responsable si un appareil personnel tel qu'un téléphone portable ou un iPad est perdu, volé ou endommagé.
- k. Signaler immédiatement tout problème de sécurité ou de sûreté, toute préoccupation en matière de confidentialité ou toute situation inappropriée ou inconfortable impliquant la technologie.
- l. Respecter les informations/médias obtenus sur Internet en incluant les références/citant la source correcte.

Surveillance et accès

Le personnel peut accéder aux comptes et communications des élèves fournis par le Conseil scolaire francophone provincial à des fins d'évaluation, pour maintenir l'intégrité du système et pour s'assurer que les élèves utilisent le système de manière responsable et sécurisée.

Conséquences

L'utilisation des ressources technologiques, y compris les réseaux, les ordinateurs ou les appareils mobiles et Internet, est un privilège qui peut être restreint ou refusé à tout moment en cas d'utilisation abusive ou de conduite abusive. Les élèves peuvent faire l'objet de mesures disciplinaires pour avoir utilisé la technologie en violation des politiques départementales, pouvant aller jusqu'à la suspension. Pour plus d'informations, consultez la Politique d'utilisation acceptable de la technologie.

2. Les outils numériques de base pour l'année scolaire 2025-2026

À lire par la famille avant de signer l'entente

Cher parent ou tuteur,

Afin d'améliorer l'apprentissage des élèves, le Conseil scolaire francophone provincial offre l'accès à des logiciels éducatifs qui répondent à nos normes élevées de sécurité en ligne. Ces outils numériques ont été approuvés par le processus de révision de la confidentialité/sécurité du Conseil scolaire francophone provincial. Ce processus assure la conformité avec la législation sur [l'Access to Information and Protection of Privacy](#), la [Schools Act 1997](#) et notre politique de confidentialité.

Les informations personnelles utilisées par les outils numériques de base énumérés ci-dessous incluent le nom de votre enfant, son adresse courriel, sa photo de profil et peuvent inclure son niveau scolaire et son école. Ces outils respectent les normes de sécurité actuelles, sont privés par défaut et l'élève conserve la propriété de tout matériel créé. Les programmes logiciels ne louent ni ne vendent les informations des utilisateurs et n'affichent pas de publicités aux utilisateurs.

Google Workspace for Education est la suite principale d'outils numériques pour soutenir l'apprentissage, la collaboration et la productivité de la maternelle à la 12e année. Cet ensemble d'outils Google inclut Classroom, Meet, Drive, Docs, Slides, Forms, et autres. [Avis de confidentialité Google Workspace for Education](#)

Microsoft 365 pour l'Éducation est une suite d'outils numériques pour les élèves de la maternelle à la 12e année qui inclut Word, PowerPoint, OneNote et Immersive Reader. [Énoncé de confidentialité Microsoft](#)

Texthelp Read & Write est une application de technologie d'assistance qui offre la conversion voix-texte, texte-voix, la traduction linguistique et une grande variété de soutiens supplémentaires aux élèves de la maternelle à la 12e année.

Texthelp EquatIO est une application de technologie d'assistance qui soutient les apprenants en mathématiques et en sciences de la maternelle à la 12e année. [Privacy Policy for Texthelp Products](#) (en anglais seulement).

Canva pour Education est une plateforme de création médiatique pour les élèves de la maternelle à la 12e année permettant de créer des présentations, affiches, bulletins d'information, vidéos, infographies, et bien plus encore. [Politique de confidentialité de Canva](#)

SMART Lumio est une plateforme d'apprentissage qui soutient l'apprentissage en présentiel ou autonome pour les élèves de la maternelle à la 12e année à partir de leçons interactives utilisant l'évaluation formative et des fonctionnalités collaboratives. [Politique de confidentialité de SMART Lumio](#)

Book Creator est un outil pour les élèves de la maternelle à la 12e année permettant de créer des livres numériques multimédias dans toutes les matières en utilisant du texte, de l'audio, de la vidéo, des dessins et des photos. [Politique de confidentialité de Book Creator](#)

Outils numériques de base supplémentaires

D'autres outils numériques peuvent être approuvés au cours de l'année scolaire, y compris ceux qui se connectent aux systèmes Google Workspace ou Microsoft 365. Tous ces outils seront examinés selon le même processus de révision de confidentialité/sécurité pour s'assurer qu'ils répondent ou dépassent les exigences de confidentialité/sécurité pour les outils numériques de base. Les parents/tuteurs seront informés si une école choisit d'utiliser ces applications.

Autres outils approuvés

Vous pouvez recevoir des formulaires de consentement supplémentaires au cours de l'année scolaire si une école choisit d'utiliser des outils nécessitant des informations personnelles supplémentaires par rapport à ce qui est couvert par ce formulaire.

Toute question ou préoccupation concernant ces logiciels éducatifs doit être adressée à l'équipe administrative de votre école.

ENTENTE

Utilisation acceptable de la technologie et des outils numériques de base

À remplir et à retourner à l'école

École: _____

NIVEAU : ● M-3e ● 4e-6e ● 7e-9e ● 10e-12e

Les parents/tuteurs devront compléter une entente mis à jour à chaque année scolaire (Primaire M-3e ; Élémentaire 4e-6e ; Intermédiaire 7e-9e ; Secondaire 10e-12e), ou lors de l'inscription dans une nouvelle école.

Parent/Tuteur

J'ai examiné les politiques décrites dans l'Entente et je comprends que mon enfant sera responsable de suivre les directives lors de l'utilisation des appareils électroniques pendant l'école et les cours. J'ai lu et discuté des directives avec mon enfant et il/elle comprend les attentes et les conséquences en cas de non-respect de l'utilisation acceptable de la technologie. Je comprends que si je souhaite retirer mon consentement pour toutes ou certaines activités à tout moment, je devrai contacter le directeur de l'école.

Toute adresse e-mail d'un élève du Conseil scolaire francophone provincial est visible, et donc accessible, à toute personne connectée à un compte e-mail d'élève en entrant le nom de l'élève. Veuillez vous assurer que votre élève se déconnecte de son compte e-mail lorsqu'il n'est pas utilisé pour empêcher un accès non autorisé par une autre personne. Les comptes e-mail des élèves doivent être utilisés uniquement à des fins éducatives.

(Veuillez cocher tout ce qui s'applique)

- Réseau local de l'école, compte e-mail, outils en ligne utilisant des ordinateurs de bureau, ordinateurs portables et appareils mobiles appartenant à l'école

Nom du parent/tuteur : _____

(En lettres moulées)

Signature : _____

Date : _____

Élève

Je comprends et je respecterai les directives d'utilisation des appareils électroniques pendant l'école et les cours. Je comprends que je pourrais perdre mes privilèges technologiques en enfreignant l'Entente pour l'utilisation acceptable de la technologie et, selon le code de conduite de mon école, des mesures disciplinaires pourraient être prises.

Nom de l'élève : _____

Niveau de l'élève : _____

(En lettres moulées)

Signature : _____

Date : _____

Cette information est collectée dans le but de s'assurer que le consentement parental est enregistré pour l'utilisation des appareils électroniques, l'utilisation de la technologie concernant les outils Web 2.0 et les applications informatiques et les appareils mobiles. Cette information est collectée en vertu de la *Loi de 1997 sur les écoles*. Pour plus d'informations, veuillez contacter la direction d'école.