

VOILE TECHNOLOGIQUE

WWW.CSF.BC.CA

CONSEIL SCOLAIRE FRANCOPHONE
DE LA COLOMBIE-BRITANNIQUE



FRANCOPHONE EDUCATION
AUTHORITY OF BRITISH COLUMBIA

180-10200 Shellbridge Way, Richmond, (C.-B.) V6X 2W7
Tél. : (604) 214-2600 | Téléc. : (604) 214-9881 | Numéro sans frais : 1-888-715-2200
info@csf.bc.ca



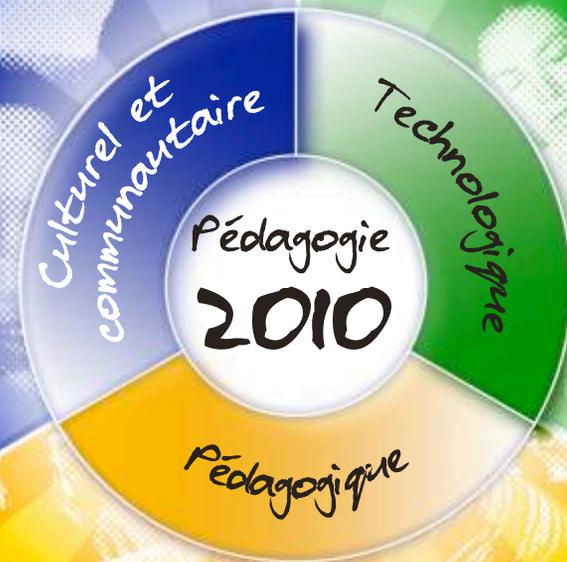
CONSEIL SCOLAIRE FRANCOPHONE
DE LA COLOMBIE-BRITANNIQUE



VOILE TECHNOLOGIQUE

LA FIERTÉ FRANCOPHONE S'APPREND AUSSI À L'ÉCOLE

CAHIER DE PROCÉDURES ET LIGNES DIRECTRICES



WWW.CSF.BC.CA

L'UTILISATION DES RESSOURCES INFORMATIQUES ET DU RÉSEAU DE TÉLÉCOMMUNICATION

Préparé par le groupe de travail en technologie du CSF

180-10200 Shellbridge Way, Richmond, (C.-B.) V6X 2W7 | (604) 214-2600 | 1-888-715-2200 | info@csf.bc.ca



Préface

Déploiement des portables



Dans le cadre du projet Pédagogie 2010, projet visant le développement et la réussite des élèves par la transformation des écoles, le CSF a commencé la première phase de déploiement d'ordinateurs portatifs dans ses écoles. Le CSF croit fortement qu'une utilisation adéquate des technologies dans l'enseignement influencera positivement la motivation des élèves envers l'apprentissage, et rendra possible d'autres formules de travail en équipe ou individualisé. Le projet contribuera aussi à la fidélisation de notre clientèle scolaire et constituera un appui de taille au personnel enseignant, brisant ainsi l'isolement des élèves tout en leur permettant de communiquer entre eux et de puiser dans une banque quasi illimitée de ressources de qualité qui ne seraient pas accessibles autrement.

Le CSF reconnaît l'importance pour son personnel, pour les élèves, jeunes et adultes, ainsi que leurs parents, d'avoir accès à ses ressources informatiques et à son réseau de télécommunication. Il demande que les objectifs pédagogiques et administratifs ainsi que ses institutions soient respectés en ce qui concerne l'utilisation de ces ressources.

Selon les procédures et politiques concernant l'utilisation des ressources informatiques et du réseau de télécommunication, le CSF, à titre de propriétaire et gestionnaire de ses ressources informatiques et du réseau de télécommunication, a le devoir de s'assurer que leur utilisation soit conforme à la légalité et respecte certaines politiques, règles et procédures. Le CSF s'attend aussi à ce que chacun des usagers se conforme aux règles usuelles de bienséance et de courtoisie de même qu'aux lois et règlements en vigueur.

Les ressources informatiques sont mises à la disposition des usagers pour la réalisation d'activités d'enseignement, d'apprentissage, de gestion, d'administration et de services à la collectivité reliés à la réalisation de la mission du CSF et ce, dans l'exercice des fonctions de chacun des usagers.

Les parents qui ont des enfants dans une classe déployée doivent prendre connaissance de l'entente MacBook pour Parent-Élève.



Préface



Aide-mémoire



Table des Matières



Présentation



Ressources

CE CAHIER APPARTIENT À

Nom : _____

Adresse : _____

Ville : _____ Province : _____

Code postal : _____ Téléphone : _____

Courriel : _____

École : _____ Division : _____

Cette entente soutient en outre que :

- L'élève s'engage à utiliser son MacBook à l'école uniquement pour ce qui se rapporte aux études.
- L'élève s'engage à ne pas installer ou télécharger d'applications sans la permission de son enseignant.
- L'élève comprend que les règlements sont expliqués dans le code de conduite de l'élève et sont stricts sur l'usage du langage ou d'images obscènes.
- L'élève s'engage à ne pas copier ou distribuer des matériels sujets aux droits d'auteurs autres que les copies de sauvegarde dont il est titulaire.
- Le parent s'engage à défrayer les coûts de la franchise en cas de perte ou dommage du portable.
- Le parent reconnaît que toute évidence en matière de vol frauduleux sera dirigée à la police et à la compagnie d'assurance aux fins de poursuites.
- Le parent et l'enfant reconnaissent qu'ils doivent se conformer au guide de conduite tel que formulé dans le Contrat parent-élève en matière de portable et de son usage (y compris le Guide TICE) selon les directives du Code3 de conduite du CSF.

Les employés du CSF ont accès aux ressources informatiques du Conseil et en contrepartie, dans l'utilisation de ces ressources :

- L'employé s'engage à respecter les personnes et leur vie privée et à ne pas communiquer de renseignements personnels concernant une autre personne;
- L'employé s'engage à ne pas télécharger ou diffuser des propos ou des images de nature offensante, diffamatoire, discriminatoire, haineuse, violente, indécente ou raciste;
- L'employé s'engage à ne pas télécharger ou diffuser des propos ou des images pouvant nuire à la réputation d'une autre personne, à celle du CSF, de ses écoles et de ses centres;
- L'employé s'engage à ne pas utiliser les équipements informatiques à des fins de publicité, de propagande, de harcèlement ou de menace;
- L'employé s'engage à respecter le droit d'auteur et à éviter de participer à des activités de piratage, notamment par la reproduction illégale de musique, jeux, logiciels et fichiers;
- L'employé s'engage à respecter les mesures de sécurité établies par le CSF et à éviter tout acte d'intrusion pouvant nuire au bon fonctionnement ou pouvant endommager les équipements informatiques du CSF ou autres;
- L'employé s'engage à éviter de poser des gestes visant à introduire et propager des virus, à modifier ou détruire sans autorisation des données ou des fichiers;
- L'employé s'engage à respecter la confidentialité des codes d'accès et des mots de passe et à éviter tout geste visant à connaître le code d'accès ou le mot de passe d'une autre personne;

- L'employé s'engage à ne pas transmettre du courrier non désiré, du courrier anonyme ou au nom d'une autre personne, ou de participer à des chaînes de lettres;
- L'employé s'engage à ne pas installer de programmes sans l'autorisation de l'administrateur du centre, du coordinateur des services technologiques, ou du conseiller pédagogique du CSF;
- L'employé s'engage à éviter toute activité illégale, contraire à la Politique d'utilisation des ressources informatiques et du réseau de télécommunications du CSF, ou qui serait incompatible avec la mission de l'école ou du centre.



Remerciements

Nous aimerions remercier spécialement la commission scolaire Eastern Townships.

Le Conseil scolaire francophone et la commission scolaire Eastern Townships ont signé une entente de partenariat afin de favoriser le partage d'expériences dans le domaine de l'apprentissage et de travailler ensemble au projet de Pédagogie 2010. Le CSET ont déjà, quant à eux, déployé plus de 12 000 portables dans les quatre dernières années.

Les membres du groupe de travail en technologie du CSF.

- | | | |
|----------------------|------------------------|----------------|
| - Martine Joseph | - Josée Bureau | - Alain Rondel |
| - Brigitte Couturier | - Marie-Claude Gilbert | - Joëlle Joly |
| - Denise Bourassa | - Denis Gendron | - Éric Leclerc |
| - Alain Thibeault | - Catherine Foisy | |



Aide-mémoire



Protection !

Lorsque tu utilises la messagerie instantanée, ne parle jamais à des inconnus et ne donne aucun renseignement personnel. Les amis virtuels peuvent souvent mentir sur leur profil.



Danger !

Lorsque tu navigues sur Internet, ne télécharge jamais des fichiers sans l'approbation de ton enseignant. Ces fichiers pourraient cacher des logiciels-espions pouvant nuire au bon fonctionnement de ton portable.



Méfiance !

Savais-tu qu'un pourriel est un courriel destiné à te faire acheter des choses inutiles ou à t'attirer sur des sites suspects ? Ne te laisse jamais tenter par ce genre de messages et supprime-les sur-le-champ.



Prudence !

Ne diffuse jamais de vidéos de toi ou d'autres personnes sur Internet.



Attention !

Ne partage jamais ton mot de passe, même pas avec tes meilleurs amis.



Table des Matières



1.0 Définitions

- 1.1 ADMINISTRATRICE OU ADMINISTRATEUR
- 1.2 RESSOURCES INFORMATIQUES
- 1.3 USAGER
- 1.4 DROIT D'AUTEUR
- 1.5 ŒUVRE
- 1.6 RENSEIGNEMENT PERSONNEL
- 1.7 TÉLÉCHARGEMENTS

2.0 Objectifs

3.0 Considérations Générales

- 3.1 PRIVILÈGE
- 3.2 PRIORITÉS
- 3.3 USAGE À DES FINS PERSONNELLES
- 3.4 CODE D'ÉTHIQUE
- 3.5 COMPORTEMENTS INTERDITS
- 3.6 MODIFICATION OU DESTRUCTION
- 3.7 ACTES PRÉJUDICIALES
- 3.8 ACCÈS NON AUTORISÉ
- 3.9 UTILISATION CONVENABLE

4.0 Droit d'Auteur et Propriété Intellectuelle

- 4.1 RÈGLE GÉNÉRALE
- 4.2 COPIES DE LOGICIELS, PROGICIELS ET DIDACTICIELS
- 4.3 COMPORTEMENTS INTERDITS

5.0 Courriel

- 5.1 IDENTIFICATION
- 5.2 RESPECT DE LA CONFIDENTIALITÉ ET DE L'INTÉGRITÉ DES MESSAGES
- 5.3 COMPORTEMENTS INTERDITS

6.0 Confidentialité et Protection des Renseignements Personnels

- 6.1 RENSEIGNEMENTS CONFIDENTIELS
- 6.2 OBLIGATIONS DE L'USAGER
 - 6.2.1 Respect des mécanismes de protection
 - 6.2.2 Diffusion de renseignements personnels
- 6.3 DROIT D'UN USAGER À LA CONFIDENTIALITÉ

7.0 Responsabilités

- 7.1 PERTE, DOMMAGE OU INCONVÉNIENT
- 7.2 ACTE ILLÉGAL
- 7.3 UTILISATION ET ENTRETIEN DE L'ÉQUIPEMENT

8.0 Urgence et Mesures de Sécurité

- 8.1 VÉRIFICATION
- 8.2 SUSPENSION DU DROIT D'ACCÈS DURANT UNE VÉRIFICATION
- 8.3 SÉCURITÉ

9.0 Sanctions

- 9.1 PÉNALITÉS ET SANCTIONS
- 9.2 IMPOSITION DES SANCTIONS

10.0 Collaboration

11.0 Responsable de l'Application et de la Diffusion de la Politique

12.0 Entrée en Vigueur

Présentation



1.0 Définitions

Dans cette politique, à moins que le contexte n'impose un sens différent, les expressions et les termes suivants signifient :

1.1 ADMINISTRATRICE OU ADMINISTRATEUR DE RÉSEAU

Toute personne au service du CSF exerçant le contrôle et la gestion d'une partie ou de l'ensemble des ressources informatiques du réseau de télécommunication.

1.2 RESSOURCES INFORMATIQUES

Sans limiter la généralité de cette expression, tous les serveurs, les ordinateurs, les postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emménagement, de reproduction, d'impression, de transmission, de réception et de traitement de l'information et tout équipement de télécommunication incluant les équipements de téléphonie, les logiciels, progiciels, didacticiels, banques de données et d'information (textuelle, sonore, graphique ou visuelle) placés dans un équipement ou sur un média informatique, système de courrier électronique, système de vidéoconférence, système de cyberconférence, système de messagerie vocale ou sur un site Web, et tout réseau interne ou externe de communication informatique dont le CSF est propriétaire ou locataire, qu'il contrôle ou administre ou sur lesquels il possède un droit d'utilisation.

1.3 USAGER

Membre du personnel, élève jeune ou adulte, parent d'élève, bénévole ainsi que toute personne physique ou morale appelée ou autorisée à utiliser les ressources informatiques.

1.4 DROIT D'AUTEUR

Signifie tous les droits conférés par la Loi sur le droit d'auteur. Il s'agit notamment du droit exclusif du titulaire de ce droit de publier, produire, reproduire, représenter ou exécuter en public, par télécommunication ou autrement, de traduire ou d'adapter sous une autre forme son œuvre ou une partie importante de celle-ci, ou de permettre à une personne physique ou morale de le faire. Poser l'un ou l'autre de ces gestes sans le consentement du titulaire du droit constitue une violation du droit d'auteur.

1.5 ŒUVRE

Signifie notamment toute œuvre littéraire, dramatique, musicale ou artistique, banque de données ou d'information (textuelle, sonore, graphique ou visuelle), prestation d'un spectacle ou toute autre œuvre visée par la Loi sur le droit d'auteur, que cette œuvre soit fixée sur un support conventionnel (livre, bande sonore, vidéocassette) ou sur un support informatique (disquette, cédérom, logiciel, disque dur) ou accessible par Internet.

1.6 RENSEIGNEMENT PERSONNEL

Renseignement qui concerne une personne physique et qui permet de l'identifier, et ce, conformément aux dispositions de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

1.7 TÉLÉCHARGEMENTS

Transfert de données par l'intermédiaire d'un réseau informatique ou par périphériques (disques externes, CD-ROM, DVD et disque image)

2.0 Objectifs

La présente politique établit les conditions d'utilisation des ressources informatiques par les usagers et vise à :

- *promouvoir une utilisation responsable des ressources informatiques;*
- *contribuer à la réalisation de la mission éducative de responsabilisation sociale des élèves;*
- *préserver la réputation du Conseil scolaire francophone comme organisme éducatif responsable;*
- *prévenir une utilisation abusive ou illégale des ressources informatiques de la part des usagers;*
- *assurer la protection des renseignements personnels;*
- *délimiter les balises touchant la vie privée des usagers dans leur utilisation des ressources informatiques;*
- *minimiser les risques de destruction ou de modification des systèmes et des données.*



3.0 Considérations Générales

3.1 PRIVILÈGE

L'accès aux ressources informatiques constitue un privilège et non pas un droit.

Seuls les usagers dûment autorisés peuvent avoir accès et utiliser les ressources informatiques, et ce, dans les limites de l'autorisation accordée à l'utilisateur par le CSF.

L'utilisateur ne peut permettre qu'un tiers non autorisé utilise ces ressources.

Les ressources informatiques doivent être utilisées de façon raisonnable et leur usage ne doit pas avoir pour effet de limiter indûment l'accès aux autres usagers.

3.2 PRIORITÉS

Les ressources informatiques sont mises à la disposition des usagers pour la réalisation d'activités d'enseignement, d'apprentissage, de gestion, d'administration et de services à la collectivité reliés à la réalisation de la mission du CSF et ce, dans l'exercice des fonctions de chacun des usagers.

3.3 USAGE À DES FINS PERSONNELLES

Les usagers peuvent utiliser les ressources informatiques du CSF à des fins personnelles à certaines conditions, notamment :

- l'utilisation n'entrave pas la performance au travail de l'employé ou celle des autres employés;
- l'utilisation n'entrave pas l'activité pédagogique des autres usagers
- l'utilisateur paie, le cas échéant, les frais d'utilisation des équipements et du matériel consommé;
- l'utilisateur respecte les dispositions de la présente politique, et ce, même s'il fait usage des ressources informatiques à des fins personnelles.

Les usagers doivent savoir que le CSF peut avoir accès aux communications ou transactions faites au moyen de ses ressources informatiques et que, par conséquent, toute utilisation à des fins personnelles ne peut aucunement être considérée comme privée.

3.4 CODE D'ÉTHIQUE

L'utilisateur des ressources informatiques agit :

- dans le respect des personnes, de leur vie privée, des renseignements personnels ou confidentiels les concernant, et ce, tant dans la communication de messages que d'images;

- dans le respect des orientations du CSF;
- dans le respect du droit d'auteur et de la propriété intellectuelle des autres;
- dans le respect des mesures de sécurité établies par le CSF;
- en se conformant aux règles de la netiquette ou guide TICE.

3.5 COMPORTEMENTS INTERDITS

Toute utilisation des ressources informatiques du CSF à des fins non autorisées ou illégales est strictement interdite. Il est interdit notamment :

- de télécharger, de stocker et de diffuser des fichiers contenant des propos ou des images de nature grossière, diffamatoire, offensante, perturbatrice, dénigrante, ou à caractère discriminatoire basé sur la race, couleur, sexe, orientation sexuelle, état civil, religion, convictions politiques, langue, origine ethnique ou nationale, condition sociale ou handicap de quiconque;
- de télécharger, de stocker et de diffuser des fichiers contenant des propos ou des images de nature haineuse, violente, indécente, pornographique, raciste ou de quelque manière illégale ou incompatible avec la mission éducative du CSF ou celle de ses écoles;
- d'utiliser les ressources informatiques à des fins de propagande, de harcèlement ou de menace sous quelque forme que ce soit, ou pour jouer un tour à des tiers (TAXAGE);
- d'utiliser les ressources informatiques pour transmettre de la publicité, faire la promotion ou effectuer des transactions dans le cadre d'un commerce personnel;
- de participer à des jeux d'argent et de paris, de quelque nature que ce soit;
- de participer à des activités de piratage (de musique, jeux, logiciels, etc.), et d'intrusion ou de blocage de systèmes informatiques de toute personne physique ou morale;
- d'utiliser les ressources informatiques pour nuire à la réputation de toute personne physique ou morale, ou du CSF.
- d'associer des propos personnels au nom du CSF dans des groupes de discussion, des séances de clavardage, ou d'utiliser tout autre mode d'échange d'opinion de manière à laisser croire que les opinions qui y sont exprimées sont sanctionnées par le CSF ou de ses écoles, sauf lorsque cela est fait par une personne autorisée à le faire dans l'exercice de ses fonctions ;
- de participer à des jeux collectifs sur Internet sauf si cette participation s'inscrit dans le cadre d'une activité pédagogique ou parascolaire étroitement supervisée et qu'elle se déroule dans un contexte assurant la sécurité des ressources informatiques et du réseau.

Les comportements interdits énumérés dans cette politique précisent les gestes qui contreviendraient à l'éthique souhaitée par le CSF dans l'utilisation des ressources



informatiques. Cependant cette énumération ne doit pas être considérée comme étant exhaustive.

3.6 MODIFICATION OU DESTRUCTION

Toute modification ou destruction des ressources informatiques est interdite sans l'autorisation de l'autorité compétente.

3.7 ACTES PRÉJUDICIALES

Il est strictement interdit de poser tout acte pouvant nuire au bon fonctionnement des ressources informatiques, entre autres, par l'insertion ou la propagation de virus informatiques, par la destruction ou la modification non autorisée de données ou de logiciels, par l'utilisation non autorisée du code d'accès ou du mot de passe d'un autre usager, ou par des gestes visant à désactiver, défier ou contourner n'importe quel système de sécurité du CSF.

3.8 ACCÈS NON AUTORISÉ

À moins d'y être autorisé, il est interdit d'accéder ou de tenter d'accéder à des fichiers, banques de données, systèmes, réseaux internes ou externes dont l'accès est restreint ou limité à une catégorie spécifique d'utilisateurs.

3.9 UTILISATION CONVENABLE

Dans un contexte de partage équitable des ressources, l'utilisateur ne doit ni monopoliser ni abuser des ressources informatiques. Il est strictement interdit d'utiliser, entre autres, en effectuant un stockage abusif d'information ou en utilisant l'Internet et son article pour écouter la radio ou une émission de télévision ou tout autre téléphonie, et ce, en dehors du contexte d'une activité pédagogique.

4.0 Droit d'Auteur et Propriété Intellectuelle

4.1 RÈGLE GÉNÉRALE

En tout temps, l'utilisateur doit respecter le droit d'auteur et les autres droits de propriété intellectuelle des tiers.

Les documents suivants sont des exemples de documents qui sont susceptibles d'être protégés par le droit d'auteur ou autres droits de propriété intellectuelle : le contenu de

courrier électronique, le contenu textuel, graphique et sonore d'un site Web, la musique et les émissions de radio et de télévision transmises par un site Web, la musique, photos ou graphismes disponibles sur le Web, les logiciels téléchargés à partir d'un site FTP, les compilations disponibles sur un site Web, l'utilisation d'un logo et d'une marque de commerce.

Dans certaines circonstances, les actions suivantes peuvent contrevenir au respect du droit d'auteur ou des droits de propriété intellectuelle :

- télécharger un fichier,
- numériser un document imprimé,
- retoucher une photographie ou le texte d'un tiers,
- diffuser de la musique sur le Web,
- afficher l'œuvre artistique d'un tiers, et ce, lorsque ces œuvres sont protégées par le droit d'auteur.

4.2 COPIES DE LOGICIELS, PROGICIELS ET DIDACTICIELS

Les reproductions de logiciels, de progiciels ou de didacticiels ne sont autorisées qu'à des fins de copies de sécurité ou selon les normes de la licence d'utilisation les régissant.

4.3 COMPORTEMENTS INTERDITS

Il est strictement interdit aux utilisateurs :

- d'utiliser toute reproduction illicite d'un logiciel ou d'un fichier électronique;
- de participer directement ou indirectement à la reproduction illicite d'un logiciel ou d'un fichier électronique;
- de modifier ou détruire un logiciel, une banque de données ou un fichier électronique, ou d'y accéder sans l'autorisation de son propriétaire;
- de reproduire la documentation associée à un logiciel sans l'autorisation du titulaire du droit d'auteur de ce logiciel;
- d'utiliser les ressources informatiques afin de commettre ou de tenter de commettre une infraction aux lois régissant le droit d'auteur et la propriété intellectuelle.
Ministère de la Justice Canada, Loi sur le droit d'auteur (L.R., 1985.C-42)
- <http://lois.justice.gc.ca/fr/frame/cs/C-42//fr>

5.0 Courriel

5.1 IDENTIFICATION

Pour tout message électronique diffusé sur le réseau du CSF, l'utilisateur doit s'identifier à titre de signataire de son message et préciser, s'il y a lieu, à quel titre il s'exprime.

5.2 RESPECT DE LA CONFIDENTIALITÉ ET DE L'INTÉGRITÉ DES MESSAGES

L'utilisateur doit respecter, lorsqu'il y a lieu, 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.

5.3 COMPORTEMENTS INTERDITS

Il est strictement interdit aux usagers :

- d'utiliser un ou des subterfuges ou d'autres moyens pour transmettre un courrier électronique de façon anonyme ou en utilisant le nom d'une autre personne;
- de s'abonner à des listes d'envoi n'ayant aucun rapport avec la fonction de l'utilisateur;
- d'expédier, sans autorisation, à tout le personnel ou à des groupes de membres du personnel, des messages sur des sujets d'intérêt divers, des nouvelles de toutes sortes, des lettres en chaîne et toute information non pertinente aux activités du CSF ou de ses écoles.

6.0 Confidentialité et Protection des Renseignements Personnels

6.1 RENSEIGNEMENTS CONFIDENTIELS

L'information contenue dans les ressources informatiques est confidentielle lorsqu'elle a le caractère d'un renseignement personnel ou d'un renseignement que le CSF protège en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, ou le caractère d'un renseignement relatif à la vie privée de la personne au sens du Code civil de la C.-B.

6.2 OBLIGATIONS DE L'USAGER

6.2.1 Respect des mécanismes de protection

L'utilisateur doit respecter les règles édictées par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, quant à la sauvegarde, l'accès, la transmission et la diffusion des renseignements personnels, et ce, au moyen de ses ressources informatiques. Loi sur l'accès à l'information (L.R., 1985, ch. A-1) <http://lois.justice.gc.ca/fr/A-1/index.html>

6.2.2 Diffusion de renseignements personnels

L'utilisateur ne peut, sans le consentement des personnes concernées, diffuser des renseignements personnels sous forme de renseignements écrits, de photographies ou autres documents visuels montrant les personnes participant à des activités permettant de les identifier de façon nominative.

L'utilisateur, lorsqu'il s'agit d'un élève, doit être informé des comportements à adopter dans la transmission des renseignements personnels le concernant ou concernant des membres de sa famille, des amis ou autre personne.

Ministère de la Justice Canada, Loi sur le droit d'auteur (L.R., 1985, Ch. P-21)
<http://lois.justice.gc.ca/fr/frame/cs/P-21//fr>

6.3 DROIT D'UN USAGER À LA CONFIDENTIALITÉ

Le CSF respecte la vie privée des usagers. Toutefois, du fait que les ressources informatiques sont mises à la disposition des usagers pour contribuer à la réalisation de la mission du CSF et celle de ses écoles, le droit à la vie privée de l'utilisateur est limité. Ainsi, les équipements,

systèmes et fichiers de travail doivent être accessibles en tout temps par la direction, tout employé suppléant ou l'administratrice ou l'administrateur du réseau.

Le CSF ne contrôlera pas systématiquement les communications des usagers. Un contrôle aura lieu seulement s'il y a raison de croire que les systèmes sont utilisés de façon inappropriée ou s'il est nécessaire de le faire dans le but de retracer une information qui ne serait autrement disponible.

L'utilisateur perd son droit à la confidentialité des fichiers qu'il a créés lorsqu'il utilise les ressources informatiques y compris toute information incluse en contravention à la présente politique ou à des directives émises par le CSF pour en assurer l'application ou à des ententes ou protocoles pertinents du CSF, ou aux lois et règlements provinciaux ou fédéraux.

L'utilisateur doit savoir que le CSF peut être appelé, dans le cadre d'une procédure judiciaire, à fournir en preuve le contenu de tout document sauvegardé sur des supports informatiques qu'elle détient. Dans un tel cas, le CSF se réserve le droit et la possibilité d'entrer dans n'importe quel système sans préavis, et d'inspecter et de contrôler toutes les données qu'il contient.

7.0 Responsabilités

7.1 PERTE, DOMMAGE OU INCONVÉNIENT

Le CSF n'assume aucune responsabilité, directe ou indirecte, pour les pertes, dommages ou inconvénients causés aux usagers à l'occasion ou en conséquence de l'utilisation des ressources informatiques, ou advenant le cas où elle devait, pour quelque cause que ce soit, diminuer ses services, ou les interrompre, quelle que soit la durée de telles diminutions ou interruptions, ou encore arrêter définitivement ses services.

7.2 ACTE ILLÉGAL

L'utilisateur est responsable des actes qu'il pose en utilisant les ressources informatiques du CSF. L'utilisateur qui commet un acte illégal s'expose à une poursuite judiciaire et à une réclamation en dommages.

7.3 UTILISATION ET ENTRETIEN DE L'ÉQUIPEMENT

Le CSF assume la responsabilité de l'utilisation et de l'entretien de l'équipement.

8.0 Urgence et Mesures de Sécurité

8.1 VÉRIFICATION

Le CSF se réserve le droit de tenir un registre des transactions effectuées avec ses ressources informatiques et son réseau de télécommunication et celui d'analyser l'information contenue dans ce registre afin de détecter les activités non autorisées, illicites ou illégales sur son réseau.

L'administratrice ou l'administrateur peut procéder à toute vérification sans préavis lorsqu'une situation d'urgence le justifie, par exemple, la détection de la présence d'un virus dans le réseau ou une surutilisation des ressources du réseau et conserver toutes copies de documents, données ou information pour s'assurer du respect des dispositions de cette politique et des directives et règles émises par le CSF.

Le CSF se réserve le droit de supprimer de ses ressources informatiques tout contenu illégal ou qui contrevient aux dispositions de la présente politique.

8.2 SUSPENSION DU DROIT D'ACCÈS DURANT UNE VÉRIFICATION

Les droits d'accès d'un usager peuvent être suspendus pendant la durée d'une vérification. Une telle décision incombe au supérieur immédiat de la personne lorsqu'il s'agit d'un employé ou au directeur de l'école lorsqu'il s'agit d'un élève ou d'un parent.

8.3 SÉCURITÉ

Le secteur des services technologiques met en place les outils informatiques assurant :

- la sécurité des ressources informatiques;
- la protection contre les virus, intrusions ou altérations de données;
- la prévention des utilisations illicites.

Le directeur des services technologiques peut édicter des directives et règlements pour assurer la sécurité des ressources informatiques, et procéder périodiquement à des vérifications de sécurité.

Ressources

Sécurité sur Internet



Afin de vous assurer que vous naviguez en toute sécurité, nous vous proposons une liste de ressources utilisées et approuvées par les services de police.

Choix.org
à www.choix.org Visitez choix.org pour consulter le guide Comment initier les enfants l'Internet et autres ressources sur la sécurité sur Internet.

Web Averti
la www.webaverti.ca Ce site fournit des outils aux parents et aux éducateurs pour assurer sécurité des jeunes sur Internet.

Réseau Éducation-Médias
www.education-medias.ca Collection de ressources et d'outils de soutien pour tous ceux qui s'intéressent aux médias et à la documentation pour les jeunes.

Cyberaide.ca
www.cyberaide.ca Child Find Manitoba vise à réduire la victimisation des enfants en offrant des programmes et des services au public canadien, y compris Cybertip.ca, la ligne nationale des tuyaux pour signaler tout cas d'exploitation sexuelle en ligne des enfants.

SécuritéCanada.ca
www.securitecanada.ca Lien pour de l'information et des services sur la sécurité publique au Canada.

Nos enfants disparus
www.nosenfantstdisparus.gc.ca Site Web d'information alimenté par des partenaires policiers et gouvernementaux qui retrouvent et ramènent des enfants disparus.

CyberAverti.ca
www.cyberaverti.ca Visitez le site de la Stratégie nationale pour la protection des enfants contre l'exploitation sexuelle sur Internet ou vous y trouverez de l'information et des ressources pour les enfants, ados, parents, enseignants et intervenants.

Conseil canadien de la sécurité
www.safety-council.org

En tant que porte-parole de la sécurité au Canada, le Conseil canadien de la sécurité s'attaque aux dossiers nouveaux et d'actualité, cherche des approches dynamiques à la prévention, et fournit des informations utiles sur des sujets d'intérêt public.

Prière de noter que les sites Web suivants n'existent qu'en anglais.

LiveWires Design
www.livewires.com

This Web site has information on Internet safety issues for parents, teachers and librarians, as well as the Missing Kit, developed by LiveWires Design Ltd, to teach children how to surf the Internet safely.

CyberCops
www.cybercops.net

CyberCops is an educational, computer-based program that teaches students in Grades 7 and 8 about the risks and safety issues associated with Internet use.

Victims of Violence
www.victimsofviolence.on.ca

This organization is dedicated to the prevention of crimes against children and, in this respect, to educating children on personal safety issues.

National
www.rcmp-grc.gc.ca

GRC - Internet 101
Caporal Yvon Brault : 613-993-5281
Dana Townsend : 613-993-5952
Daniel Mulligan : 613-993-5952

Source : Gendarmerie royale du Canada