Politique d'utilisation des ressources informatiques, de la vidéosurveillance, des technologies de l'information et des médias sociaux

B)

TABLE DES MATIÈRES

OBJET : Politique d'utilisation des ressources informatiques, de la vidéosurveillance, des technologies de l'information et des médias sociaux	
UNITÉ ADMINISTRATIVE : 620 **SERVICES DES RESSOURCES INFORMATIQUES**	**IDENTIFICATION** **620-01**

PRÉAMBULE

La Commission scolaire Marguerite-Bourgeoys, ci-après la Commission, reconnaît l'importance pour ses élèves et son personnel d'avoir accès à ses ressources informatiques pour la réalisation des activités d'enseignement, d'apprentissage, de gestion et des services à la communauté reliés à sa mission. En tant que propriétaire et gestionnaire des ressources informatiques, la Commission doit s'assurer que leur utilisation ainsi que le traitement de l'information sont conformes à des règles de conduite et à une éthique dont les objectifs et les principes directeurs sont définis dans la présente politique.

La Commission reconnaît également l'importance que prennent les médias sociaux et l'intérêt que lui portent ses employés, élus, représentants, bénévoles, les élèves et leurs parents. L'utilisation de ces outils de communication nécessite des balises, lesquelles se retrouvent dans la présente politique.

La présente politique promeut une utilisation responsable des ressources informatiques et des outils de communication qui préservent la réputation de la Commission et des acteurs de sa communauté éducative, en plus de protéger leurs droits.

La présente politique précise également les rôles et responsabilités de ces acteurs en lien avec les médias sociaux.

Elle campe finalement les règles de conduite applicables et les comportements attendus, avec l'objectif de prévenir toute utilisation inadéquate de ces outils de communication. Par ailleurs, la Commission doit, en vertu de la *Loi sur l'instruction publique*, veiller à ce que chacun de ses établissements offre une milieu sain et sécuritaire de manière à ce que tout élève qui le fréquente puisse y développer son plein potentiel, à l'abri de toute forme d'intimidation ou de violence. Parmi les différents moyens mis en place pour s'en assurer, elle s'est dotée d'un système de vidéosurveillance. Ce système est utilisé dans ses établissements et édifices administratifs afin d'assurer tant la sécurité des personnes que celles des lieux. La Commission reconnaît toutefois que l'utilisation de la vidéosurveillance ne remplace par la présence d'intervenants qualifiés dans les milieux, mais constitue plutôt un moyen complémentaire à la surveillance et aux interventions déjà effectuées.

L'application de cette politique se fait conformément aux autres politiques de la Commission, dans le respect des conventions collectives, ainsi qu'avec les lois et règlements en vigueur au Québec et au Canada.

L'usage du genre masculin inclut le féminin et a été utilisé dans le seul but d'alléger le texte.

1. DÉFINITIONS

ADMINISTRATEUR

Gestionnaire d'un espace de médias sociaux, l'administrateur exerce un contrôle sur le contenu diffusé sur les pages qu'il gère. L'administrateur principal d'un espace doit être un employé de la Commission.

BLOGUE (FORUM DE DISCUSSION)

Site web tenu par un ou plusieurs blogueurs qui s'expriment librement et selon une certaine périodicité, sous la forme de billets ou d'articles, informatifs ou intimistes et datés à la manière d'un journal de bord.

CLAVARDAGE (chat)

Activité permettant à un internaute d'avoir une conversation écrite, interactive et en temps réel avec d'autres internautes par clavier interposé.

CYBERINTIMIDATION

Acte d'intimidation posé par l'intermédiaire de toute plateforme technologique, notamment les médias sociaux, les téléphones cellulaires et les courriels.

DROIT D'AUTEUR

Droit exclusif de produire ou de reproduire une œuvre ou une partie importante de celle-ci, sous une forme matérielle quelconque, de la présenter en public, de la publier, de permettre l'un des actes ci-dessus énumérés ainsi que tous les droits accessoires y afférents, le tout tel que défini par la *Loi sur le droit d'auteur*.

DROIT D'UTILISATION

Autorisation accordée à une personne définissant l'usage qu'elle peut faire des ressources informatiques.

ÉLÈVE

Toute personne, jeune ou adulte, inscrite officiellement à ce titre, dans les registres de la Commission, quel que soit le régime pédagogique qui lui est applicable.

ESPACE

Toutes formes d'application, de plateforme et de média virtuel administrés par la Commission, ses services et ses établissements exclusivement dans le domaine des réseaux sociaux.

FILTRAGE

Technologie visant à limiter l'accès à certains sites normalement accessibles sur internet.

GESTIONNAIRE DE SYSTÈME

Tout membre du personnel dont la fonction est d'assumer la responsabilité de gestion d'équipements, de ressources, de systèmes ou de réseaux au sens de la présente politique, et toute personne à qui cette responsabilité est conférée en vertu d'une entente avec la Commission.

ILLICITE

Tout élément dont le contenu est de nature haineuse, discriminatoire, indécente, pornographique, raciste, violente ou de toutes sources illégales.

INTERNET

Réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, reliés par le protocole de communication TCP-IP et coopérant dans le but d'offrir une interface unique à leurs utilisateurs.

INTIMIDATION

Tout comportement, parole, acte ou geste délibéré ou non à caractère répétitif, exprimé directement ou indirectement, y compris sur internet, dans un contexte caractérisé par l'inégalité des rapports de force entre les personnes concernées, ayant pour effet d'engendrer des sentiments de détresse et de léser, blesser, opprimer ou ostraciser.

NÉTIQUETTE

Ensemble des règles de bonne conduite et de politesse à observer sur internet, notamment lors des échanges sur les médias sociaux.

MÉDIAS OU RÉSEAUX SOCIAUX

Toutes formes d'application, de plateforme et de média virtuel en ligne visant à faciliter l'interaction sociale, la collaboration, la création ainsi que le partage et la diffusion de contenus. Les médias sociaux sur internet comprennent notamment :

- Les sites sociaux de réseautage (Facebook, LinkedIn, etc.);
- les sites de partage de vidéos ou de photographies (Facebook, Instagram, Flickr, Youtube, SnapChat, etc.);
- les sites de microblogage (par exemple Twitter);
- les blogues, personnels ou corporatifs;
- les forums de discussion (Yahoo!, Google groups, Rate my teacher, etc.);
- les encyclopédies en ligne (par exemple Wikipédia);
- tout autre site internet ou plateforme en ligne permettant à des personnes de participer à des activités de réseautage ou d'utiliser des outils de publication en ligne.

POSTE DE TRAVAIL INFORMATISÉ

Tout appareil qui peut être utilisé pour accéder, saisir, traiter ou emmagasiner des données de façon autonome ou en lien avec d'autres équipements informatiques.

RENSEIGNEMENTS PERSONNELS

Tout 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*.

RÉSEAU INFORMATIQUE

Ensemble des composantes et des équipements informatiques reliés par voie de télécommunication en vue d'accéder à des ressources ou à des services informatisés, ou de partager cet accès.

RESSOURCES INFORMATIQUES

Ordinateurs, tablettes, appareils connectés, téléphones intelligents, montres intelligentes, tableau numérique interactif et projecteurs, imprimantes, moniteurs, bornes sans-fil, serveurs et dispositifs d'emmagasinage, de reproduction, de transmission, de réception et de traitement de l'information, dont la Commission est propriétaire ou locataire ou sur lesquels elle possède un droit à l'utilisation.

UTILISATEURS

Tout employé, élu, représentant et bénévole de la Commission, ainsi que tout élève et ses parents, de même que toute autre personne utilisant les ressources informatiques de la Commission, pouvant circuler dans l'établissement ou pouvant accéder aux espaces de la Commission.

VIDÉOSURVEILLANCE

Système de caméras de surveillance avec enregistrement.

2. OBJECTIFS ET PRINCIPES

2.1 OBJECTIFS

L'objectif premier de la présente politique est d'établir le cadre réglementaire régissant l'utilisation de toute ressource informatique à la Commission.

Elle a également pour objectifs :

- de promouvoir une utilisation des médias sociaux responsable;
- de sensibiliser tout utilisateur sur l'impact ou la conséquence que peut avoir son utilisation des médias sociaux;
- de prévenir une utilisation incorrecte, abusive ou illégale des médiaux sociaux de la part des utilisateurs;
- de favoriser une utilisation adéquate et optimale des réseaux sociaux pour la réalisation d'objectifs pédagogiques ou autres;
- de protéger la réputation et l'image de la Commission, de ses employés, ses élus ou représentants ainsi que celle de ses élèves;
- de s'assurer de protéger les autres droits de ses employés, élus, représentants ainsi que ceux de ses élèves, notamment la confidentialité de leur dossier et la protection de leurs renseignements personnels;
- d'encadrer l'installation et l'utilisation de la vidéosurveillance avec enregistrement dans les établissements et les édifices administratifs;
- de protéger la vie privée et les renseignements personnels des personnes touchées par l'utilisation de la vidéosurveillance avec enregistrement dans les établissements et les édifices administratifs;

- de faire connaître à la population concernée les modalités d'utilisation de la vidéosurveillance avec enregistrement dans les établissements et les édifices administratifs;
- de protéger les investissements collectifs et les utilisateurs contre un usage abusif et illégal des ressources informatiques;
- d'assurer le respect de toute législation à l'égard de l'usage et du traitement de l'information et de l'utilisation des technologies de l'information et des communications;
- de définir les rôles et responsabilités de chacun.

2.2 PRINCIPES ET OBJECTIFS À L'ÉGARD DE L'UTILISATION DE LA VIDÉOSURVEILLANCE

La vidéosurveillance peut être utilisée pour les raisons suivantes :

- assurer la sécurité des élèves, du personnel et des membres de la communauté;
- protéger les immeubles contre le vol et le vandalisme;
- identifier les personnes avant leur entrée dans les établissements et prévenir l'accès des intrus.

2.3 PRINCIPES À L'ÉGARD DES TECHNOLOGIES DE L'INFORMATION ET DES MÉDIAS SOCIAUX

La présente politique se veut un complément de toute autre politique adoptée par la Commission dont, notamment, la *Politique pour promouvoir la civilité et pour prévenir et contrer le harcèlement psychologique en milieu de travail.*

Toute personne a droit au respect de sa vie privée ainsi que le droit à la sauvegarde de sa dignité, de son honneur et de sa réputation.

Toute personne est titulaire de libertés fondamentales telles que la liberté d'expression. Cependant, ce droit n'est pas absolu. Il ne peut en aucun moment être exercé à des fins d'atteinte à la réputation, de harcèlement, de menace et de discrimination à l'égard de quiconque.

L'utilisation des médias sociaux dans un cadre pédagogique ou professionnel est permise dans la mesure où celle-ci se fait dans le respect de la présente politique et qu'elle est autorisée par la direction de l'établissement.

L'utilisation des médias sociaux à titre personnel ne doit pas se faire en contravention de ses obligations à l'égard de la Commission et doit se faire dans le respect de la présente politique.

À titre d'employé, tout membre du personnel œuvrant auprès des élèves, exerce un rôle de modèle à l'égard de ceux-ci. Ce rôle s'exerce dans l'établissement ou à l'extérieur de celui-ci. Une attention particulière doit donc être portée lors de l'utilisation des médias sociaux.

Tout ce qui est publié sur un espace de la Commission devient public. Par conséquent, l'utilisateur ne peut en aucun temps prétendre à une expectative de vie privée. Les commentaires sur ces espaces n'engagent que leur auteur et toute contravention aux règles qui précèdent peut engager la responsabilité civile, criminelle ou pénale de ce dernier.

3. CHAMPS D'APPLICATION DE LA PRÉSENTE POLITIQUE

La présente politique s'applique :

- à tous les employés, élus, représentants et bénévoles de la Commission, ainsi qu'aux élèves et à leurs parents, de même qu'à toute autre personne utilisant les ressources informatiques de la Commission;
- à toute personne pouvant circuler dans l'établissement (parents, élèves, personnel de la Commission scolaire et citoyens);
- à l'utilisation de toute ressource informatique appartenant à la Commission, peu importe sa localisation, ou ne lui appartenant pas, mais utilisé dans ses locaux, ou relié à son réseau informatique;
- à l'utilisation de toutes données saisies, traitées ou emmagasinées à l'aide d'équipements, de systèmes ou d'autres moyens exploitant des technologies de l'information et des télécommunications que la Commission utilise pour ses activités d'enseignement et de gestion;
- pour tout usage des médias sociaux, particulièrement l'utilisation faite à l'aide des ressources informatiques de la Commission.

La présente politique ne s'applique pas :

- à une enquête administrative menée par le Service des ressources humaines ou le Secrétariat général;
- à l'utilisation de la vidéosurveillance dans les autobus scolaires.

4. RESPONSABILITÉS DE LA COMMISSION

Le Conseil des commissaires adopte la présente politique, s'assure du respect de celle-ci par ses membres et autorise les unités administratives de la Commission à agir tel que le prévoit la politique, le tout, dans le respect du Règlement de délégation de pouvoirs.

La Direction générale s'assure de l'application de la présente politique dans les établissements et les unités administratives de la Commission.

La Commission n'assume aucune responsabilité, directe ou indirecte, pour les pertes, dommages ou inconvénients causés aux utilisateurs à l'occasion ou en conséquence de l'utilisation des ressources informatiques, d'internet ou des médias sociaux sous réserve de ses obligations prévues dans les différentes lois qui lui sont applicables, notamment la *Loi sur l'instruction publique.*

5. RESPONSABILITÉS DU SERVICE DES RESSOURCES INFORMATIQUES

Étant responsable de son application, le Service des ressources informatiques informe les directions d'établissement et de service de l'existence et des implications de la présente politique.

Le Service des ressources informatiques s'assure de sa diffusion ainsi que de l'émission de modalités d'application conçues dans le but de faciliter l'application de la présente politique.

Le Service des ressources informatiques s'assure également que tout système d'information soit protégé au minimum par un processus d'accès nécessitant un mécanisme d'identification et d'authentification de l'utilisateur. Il doit en plus limiter l'accès aux personnes autorisées seulement, en fonction de la nature de l'information et des applications utilisées.

Il assure également, en collaboration avec le Bureau des communications une vigie relativement aux espaces de la Commission.

Il est responsable d'informer le personnel chargé du soutien technique des principes et des modalités prévues lors de l'utilisation de la vidéosurveillance.

En collaboration avec le service concerné, le cas échéant, il intervient auprès des utilisateurs concernés afin que les règles prévues à la présente politique soient respectées.

6. RESPONSABILITÉS DU BUREAU DES COMMUNICATIONS

Le Bureau des communications assure une vigie relativement aux espaces de la Commission.

Il analyse et autorise, le cas échéant, la mise en ligne d'un espace « Commission ».

Il analyse et autorise, le cas échéant, l'utilisation du logo de la Commission.

En collaboration avec le service concerné, le cas échéant, il intervient auprès des utilisateurs concernés afin que les règles prévues à la présente politique soient respectées.

7. RESPONSABILITÉS DES DIRECTIONS D'ÉCOLE, DE CENTRE ET DE SERVICE

La direction d'établissement ou de service est responsable de l'application de la présente politique et des modalités d'application en découlant dans son unité administrative. Elle informe les utilisateurs internes et externes sous sa responsabilité des principes et des modalités d'application de la présente politique.

La direction de chaque école, centre et service doit s'assurer que les élèves respectent les dispositions de la présente politique lors de l'utilisation des ressources informatiques.

La direction de chaque école, centre et service doit, pour tout espace propre à son établissement ou à son service, superviser l'administration et la vigie de cet espace. Elle doit également prendre les moyens raisonnables afin de sensibiliser les utilisateurs liés à son établissement sur la portée et les effets d'une adhésion à une application, une plateforme ou un média virtuel faisant partie des médias sociaux.

8. RESPONSABILITÉS DE L'ADMINISTRATEUR

L'administrateur doit être un employé de la Commission. Si plusieurs administrateurs se partagent la gestion d'un espace, l'administrateur principal doit être employé de la Commission.

L'administrateur doit obtenir, au préalable, l'autorisation de la direction pour la création d'un espace.

L'administrateur exerce un contrôle sur le contenu de tout espace qui est sous sa responsabilité et s'assure du bon fonctionnement des systèmes qui lui sont confiés. Il contrôle également l'accès et l'utilisation de ces systèmes.

Il jouit de prérogatives d'accès supérieures à celles du simple utilisateur, selon les besoins de sa tâche.

Il prend les moyens appropriés pour corriger toute situation où il y aurait contravention aux règles d'utilisation d'un système qui est sous sa responsabilité ou lorsqu'il y aurait contravention aux règles de la présente politique.

9. RESPONSABILITÉS DES UTILISATEURS

Tout utilisateur doit prendre connaissance de la présente politique. La Commission pourra lui demander de confirmer qu'il a reçu et pris connaissance de la présente politique et qu'il s'engage à la respecter.

Tout manquement à la présente politique et à ses modalités d'application doit être rapporté au directeur de l'unité administrative concernée, qui en informe la direction du Service des ressources informatiques.

L'utilisateur est responsable des actes qu'il pose en utilisant les ressources informatiques, le réseau internet et les espaces administrés par la Commission et ses établissements Conséquemment, l'utilisateur devra prendre fait et cause pour la Commission et tenir cette dernière indemne de tout jugement pouvant intervenir contre elle qui découlerait d'un acte commis par l'utilisateur.

L'utilisateur doit assumer la responsabilité de la sécurité, de l'intégrité de l'information et des traitements effectués sur les équipements qu'il utilise. Il doit protéger la confidentialité des renseignements qu'il peut détenir, soit dans le cadre de ses fonctions à titre de membre du personnel, soit dans le cadre d'une entente formelle avec la Commission à titre de client ou fournisseur, soit privément à titre personnel et, s'il y a lieu, en protéger l'accès par un mot de passe.

10. UTILISATION DES RESSOURCES INFORMATIQUES

10.1 DROIT D'USAGE ET CODE D'ACCÈS

L'utilisation des ressources informatiques de la Commission est un privilège et non un droit. Il peut être révoqué en tout temps à tout utilisateur qui ne se conforme pas à la présente politique.

Un code d'accès individuel ainsi qu'un mot de passe confidentiel sont alloués à chaque utilisateur, conformément aux modalités d'application.

L'utilisateur a l'obligation de s'identifier clairement lors de toute utilisation du réseau informatique de la Commission.

L'utilisateur est en tout temps responsable de toute forme de communication effectuée avec son code d'accès et son mot de passe. Il doit ainsi protéger son mot de passe et ne jamais le divulguer.

10.2 UTILISATION PRIORITAIRE DES ÉQUIPEMENTS

Les ressources informatiques de la Commission sont mises à la disposition des utilisateurs pour la réalisation d'activités d'enseignement, d'apprentissage, de recherche, de gestion ou à toutes autres fins autorisées par la Commission.

Dans un contexte de partage équitable des ressources, l'utilisateur doit faire un usage raisonnable des ressources informatiques de la Commission et éviter de les monopoliser ou d'en abuser entre autres, en effectuant un stockage abusif d'information.

Aucun utilisateur ne doit agir de façon à empêcher le fonctionnement normal des ressources informatiques ou 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.

Personne ne peut utiliser les ressources informatiques à des fins illicites ou illégales.

10.3 CONDITIONS D'UTILISATION

L'utilisateur doit :

- Toujours s'identifier à titre de signataire d'un message et préciser, s'il y a lieu, à quel titre il s'exprime;
- Utiliser les ressources informatiques 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;
- S'assurer que les communications faites dans le cadre de l'utilisation des ressources informatiques sont empreintes de respect et de civisme et sont faites dans un langage courtois;
- Utiliser les ressources informatiques dans le respect de la réputation et de l'image de la Commission, de ses établissements, du personnel et des élèves;
- Avant de procéder à l'installation d'un logiciel, s'assurer qu'il est autorisé, accompagné d'une licence et supporté par le Service des ressources informatiques;
- S'assurer auprès du Service des ressources informatiques que les fichiers et logiciels téléchargés ne peuvent entraver l'intégrité du réseau ni le bon fonctionnement des ordinateurs;
- Respecter les mesures de sécurité, notamment et non limitativement, les filtres internet et les coupe-feux établis par la Commission.

10.4 UTILISATION À DES FINS PERSONNELLES

Les ressources informatiques fournies par la Commission et le matériel qui s'y rattache doivent être utilisés par les membres du personnel dans l'exercice de leurs fonctions.

Par contre, à titre de privilège, les membres du personnel peuvent faire usage de certaines ressources informatiques à des fins personnelles à certaines conditions :

- l'utilisation doit se faire en dehors des heures de prestation de travail (pause ou période de repas) et ne pas entraver la performance au travail du personnel;
- l'utilisation ne nuit nullement aux opérations de la Commission, ni à l'efficacité ou à la disponibilité du système informatique;
- la durée de l'accès est limitée;
- l'utilisation n'est pas faite à des fins commerciales, lucratives, de propagande ou contraire à la loi;
- l'utilisation respecte les dispositions de la présente politique, et ce, même si l'utilisateur fait usage des ressources informatiques à des fins personnelles.

En tout temps, les informations ou communications transmises ou reçues par internet sont présumées être de nature professionnelle et concerner les affaires de la Commission. En conséquence, aucun utilisateur ne peut prétendre au caractère privé de ses échanges ou de son utilisation des ressources informatiques, le tout sous réserve des principes établis par la loi ou la jurisprudence en matière de confidentialité et de respect à la vie privée.

10.5 ACTIONS PROHIBÉES

Il est **interdit**, notamment et non limitativement :

- d'utiliser les ressources informatiques à des fins de publicité, de propagande, de harcèlement, de diffusion de propos diffamatoires et haineux, offensants, perturbants, dénigrants ou incompatibles avec la mission éducative de la Commission;
- de divulguer des renseignements personnels, incluant des photographies, sans l'autorisation **écrite** de la personne concernée ou du titulaire de l'autorité parentale;
- d'expédier des messages à tous les utilisateurs de la Commission sur des sujets d'intérêt public, des nouvelles de toutes sortes, des opinions à des fins politiques ou à des fins de propagande, des lettres en chaîne et toute information non pertinente dans le cadre du travail scolaire, pédagogique ou administratif; d'utiliser internet à des fins personnelles durant les heures de travail ou de classe à moins d'autorisation à cet effet de la part du supérieur immédiat ou du responsable pédagogique pour les élèves utilisateurs;

- de consulter, télécharger ou transférer du matériel obscène, à connotation violente ou sexuelle;

- de créer, installer, transférer, télécharger ou utiliser des fichiers informatiques n'ayant aucun rapport avec la Commission ou les fonctions du membre du personnel;

- de surcharger les systèmes informatiques par une utilisation exagérée (ex. : écouter la radio sur internet);

- de participer à des jeux de hasard, des paris ou des concours;

- de transmettre un courrier électronique de façon anonyme ou en utilisant le nom d'une autre personne;

- d'engager des frais à même les ressources de la Commission;

- 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, ou par des gestes visant à désactiver, défier ou contourner n'importe quel système de sécurité;

- d'utiliser les ressources informatiques pour nuire à la réputation et à l'image de la Commission, de ses établissements et de quiconque;

- de diffuser, stocker ou partager sur les systèmes informatiques de la Commission des éléments illicites et illégaux;

- d'utiliser des logiciels de partage de fichier (ex : Bittorrent, Gnutella, Gnutella2, eDonkey2000, DirectConnect, DC++, Mute, etc.), ces derniers contrevenant à la *Loi sur le droit d'auteur*;

- de participer à des activités de piratage (de musique, jeux, logiciels, etc.) et d'intrusion ou de blocage de système informatique;

- d'utiliser des serveurs permettant de contourner les processus de navigation internet autorisés, tels que les serveurs proxy, Tor ou VPN à des fins contraires à la présente politique.

11. UTILISATION DE LA VIDÉOSURVEILLANCE

11.1 CONDITIONS D'UTILISATION

L'utilisation de caméras de surveillance n'est autorisée que lorsque des risques concrets et des dangers réels pourraient affecter l'ordre public et la sécurité des personnes, des lieux ou des biens.

Les solutions de rechange, moins préjudiciables à la vie privée, doivent avoir été envisagées ou mises à l'essai et s'être avérées inefficaces, inapplicables ou difficilement réalisables.

Des panneaux informant les élèves, les membres du personnel et le public que les lieux sont sous surveillance vidéo doivent être placés en évidence aux entrées des édifices, sur les murs extérieurs et intérieurs.

11.2 EMPLACEMENT DES CAMÉRAS

Les caméras doivent être installées et orientées de manière à ne capter que les images des endroits qui, après analyse, sont identifiées comme nécessitant une surveillance vidéo. Elles ne doivent pas être orientées de manière à capter des images à l'intérieur des édifices voisins et, autant que possible, de leur terrain. À cette fin, la technique informatique de masquage des lieux doit être retenue pour éviter une prise de vue d'endroits privés ou d'endroits qui ne sont pas concernés par la vidéosurveillance.

Les angles de vue, le type de caméra, la fonction zoom ou l'arrêt sur image doivent être évalués en fonction des finalités recherchées et des moyens appropriés pour atteindre ces finalités.

Les caméras ne devraient jamais être installées dans les classes, à moins que, à la suite d'une demande motivée, cette installation ait été préalablement autorisée par le directeur général adjoint responsable de l'établissement concerné et le responsable de l'accès à l'information et de la protection des renseignements personnels de la Commission.

Les caméras ne doivent jamais être placées de manière à surveiller l'intérieur de pièces où les élèves, le personnel et le public s'attendent à plus d'intimité, y compris, mais sans restreindre la généralité de ce qui précède, les vestiaires et les toilettes.

11.3 ENREGISTREMENT

11.3.1 DÉLAI DE CONSERVATION

Le délai de conservation des supports d'enregistrement est pris en compte dans le calendrier de conservation.

Mis à part les exigences judiciaires et les enquêtes policières ou administratives, les enregistrements sont effacés ou détruits dans un délai de 30 jours de la captation.

11.3.2 CLASSEMENT

Les supports d'enregistrement doivent être numérotés et datés par site ayant fait l'objet d'une surveillance.

11.3.3 COUPLAGE D'INFORMATIONS

Les enregistrements ne doivent pas faire l'objet d'associations d'images et de données biométriques, notamment à l'aide de logiciels de consultation automatique d'images ou de reconnaissance faciale.

Les enregistrements ne doivent pas être appariés, couplés ou partagés avec d'autres fichiers, ni servir à constituer des banques de données.

11.3.4 CONFIDENTIALITÉ

L'utilisation de la vidéosurveillance doit se faire de manière à minimiser ses effets et à préserver le mieux possible la vie privée des élèves, du personnel et du public.

Sous réserve des exceptions prévues à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, les enregistrements ne doivent pas être communiqués à des tiers ni reproduits sur d'autres supports. Dans l'éventualité où des copies devaient être faites et conformément à cette loi, ces copies doivent être conservées dans un lieu sûr et sécuritaire.

À l'exception des caméras utilisées pour contrôler les entrées et sorties ou à moins d'avoir un motif raisonnable de croire qu'une infraction est en train ou sur le point d'être commise, les images captées par les caméras de vidéosurveillance ne doivent pas être regardées en continu par qui que ce soit.

La direction d'établissement, le secrétaire général, le responsable de l'accès aux documents et de la protection des renseignements personnels, la direction du Service des ressources informatiques ainsi que les personnes désignées par ces derniers sont les seules personnes autorisées à regarder les images captées.

11.3.5 CONNAISSANCE DES RÈGLES

Les personnes assurant le fonctionnement des appareils de vidéosurveillance doivent s'assurer du respect de la présente politique et connaître les règles visant à protéger la vie privée.

11.4 AJOUT DE CAMÉRAS

La direction d'établissement doit formuler une demande écrite d'installation de caméras de vidéosurveillance à la direction du Service des ressources informatiques. Elle doit comprendre les éléments suivants :

- la description du problème vécu;
- le nombre de caméras requis et les endroits qui seront surveillés;
- les utilisateurs autorisés à visionner les images.

12. UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DES MÉDIAS SOCIAUX

12.1 CONDITIONS D'UTILISATION

La Commission, ainsi que ses établissements ou services qui administrent des comptes sur les réseaux sociaux, doivent indiquer dans la nétiquette que l'âge minimal pour se créer un profil sur les réseaux sociaux est de 14 ans.

L'utilisateur agit dans le respect des personnes, de leur vie privée, des renseignements personnels ou confidentiels les concernant, et ce, tant dans la communication d'écrits que dans celle d'images. L'autorisation écrite préalable des personnes (ou du titulaire de l'autorité parentale s'il s'agit d'un mineur) dont des renseignements les concernant ou dont l'image (photo ou vidéo) sera diffusée devra être obtenue.

L'utilisateur agit dans le respect du droit d'auteur et de la propriété intellectuelle.

12.2 ACTIONS PROHIBÉES

Il est **interdit**, notamment et non limitativement :

- de diffuser des messages ou des fichiers contenant des propos ou des images diffamatoires, dénigrantes ou à caractère discriminatoire basés sur la race, le genre, la couleur, le sexe, l'identité ou l'expression du genre, la grossesse, l'orientation sexuelle, l'état civil, la religion, les convictions politiques, la langue, l'origine ethnique ou nationale, la condition sociale ou le handicap;

- de diffuser des messages ou des fichiers contenant des propos ou des images de nature haineuse, offensante, perturbatrice, intimidante, violente, indécente, pornographique, raciste ou de quelque manière illégale ou incompatible avec la mission éducative ou les normes administratives établies par la Commission ou avec celles de ses établissements;

- d'utiliser les médias sociaux de quelque façon que ce soit à des fins de propagande, de harcèlement, d'intimidation, de cyberintimidation ou de menace;

- d'associer, par quelque moyen que ce soit, les propos personnels au nom de la Commission ou à celui d'un établissement dans des groupes de discussion, des séances de clavardage ou d'utiliser tout autre mode d'échange d'opinions de manière à laisser croire que les propos

qui y sont exprimés sont endossés par la Commission ou par l'établissement, sauf lorsque cela est fait par une personne autorisée à le faire dans l'exercice de ses fonctions à la Commission;

- d'utiliser les médias sociaux durant les heures de prestation de travail sauf si cette activité s'inscrit dans le cadre professionnel ou d'une activité pédagogique ou parascolaire étroitement supervisée et qu'elle se déroule dans un contexte assurant la sécurité des ressources informatiques.

12.3 RÈGLES PARTICULIÈRES RELATIVES À CERTAINES CATÉGORIES D'UTILISATEURS

12.3.1 EMPLOYÉS/ÉLÈVES OU PARENTS

Les communications entre les membres du personnel et les élèves de la Commission doivent être effectuées en priorité sur des espaces administrés par la Commission, ses services ou ses établissements.

Un membre du personnel ne peut établir un lien « d'amitié » ou communiquer avec un élève par le biais des réseaux sociaux, sauf si cette communication se déroule dans un cadre scolaire. Le membre du personnel concerné devra alors en informer la direction de l'établissement. Cette interdiction n'est pas applicable à ceux qui ont un lien de parenté.

Les communications à l'aide des médias sociaux entre les membres du personnel et les élèves/ parents de la Commission doivent, en tout temps, être empreintes de courtoisie. De plus, les membres du personnel, dans le cadre de ces communications, doivent maintenir et respecter des limites professionnelles.

12.3.2 EMPLOYÉS/EMPLOYÉS

Les communications à l'aide des médias sociaux entre les membres du personnel, autres que celles strictement liées à leurs fonctions, doivent avoir lieu à l'extérieur de leur prestation de travail.

Les communications électroniques entre les membres du personnel doivent en tout temps être empreintes de courtoisie et s'inscrire à l'intérieur des balises de la présente politique.

12.3.3 EMPLOYÉS/PUBLIC

Les communications à l'aide des médias sociaux entre les membres du personnel et le public autres que celles strictement liées à leurs fonctions doivent avoir lieu à l'extérieur de leur prestation de travail.

Les communications à l'aide des médias sociaux entre les membres du personnel et le public doivent en tout temps être empreintes de courtoisie et s'inscrire à l'intérieur des balises de la présente politique.

12.3.4 ÉLÈVES/ÉLÈVES

Les communications à l'aide des médias sociaux entre les élèves de la Commission doivent être empreintes de courtoisie et doivent également s'inscrire à l'intérieur des règles établies dans la présente politique. Les communications électroniques effectuées entre les élèves doivent être traitées comme si les propos avaient été tenus dans le cadre scolaire s'ils concernent la Commission, un membre de son personnel ou un de ses élèves et doivent être traitées par les établissements concernés selon les codes de vie ou les règles de conduite en vigueur dans ces établissements, et ce, à compter du moment où la situation est portée à la connaissance du personnel ou seulement du personnel de direction, selon le contexte.

13. RESSOURCES INFORMATIQUES

13.1 PROTECTION DES RESSOURCES INFORMATIQUES

La protection des ressources informatiques relève exclusivement du Service des ressources informatiques. À cet effet, il doit instaurer des mesures de contrôle et de sécurité appropriées pour protéger adéquatement les installations sous sa responsabilité.

La protection des ressources informatiques locales et de leur contenu incombe aux unités administratives qui en sont les utilisatrices. La direction de ces unités administratives doit mettre en place les mesures de contrôle et de sécurité appropriées.

Seules les personnes dûment autorisées peuvent utiliser les ressources informatiques de la Commission.

Tout accès ou tentative d'accès non autorisé aux ressources informatiques de la Commission constitue une violation à la présente politique et doit être rapporté au directeur du Service des ressources informatiques.

13.2 INTÉGRITÉ ET PROPRIÉTÉ DES DONNÉES

L'information installée par la Commission dans les ressources informatiques de la Commission demeure la propriété de celle-ci.

Toute information ainsi que tout matériel informatique créé par tout membre du personnel dans le cadre de ses fonctions au sein de la Commission demeure la propriété de celle-ci.

La gestion de cette information doit être conforme à la « Politique de gestion des documents » de la Commission et aux déclarations de fichiers de renseignements personnels conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* y compris lors du départ ou de la réaffectation de l'employé qui en avait la garde.

Personne ne doit modifier ou détruire les données, les logiciels, la documentation et les ressources informatiques de la Commission sans l'autorisation d'un membre du Service des ressources informatiques.

Tout extrant issu de systèmes informatisés ou de télécommunications et contenant de l'information confidentielle doit être conservé de façon sécuritaire, et détruit selon les normes de confidentialité, et éventuellement d'archivage, lorsque sa détention ou son utilisation n'est plus nécessaire.

La Commission se réserve le droit de conserver ou de retenir certaines informations transmises à l'aide de ses ressources informatiques, au même titre que la conservation de certaines informations imprimées sur support papier ou avec l'équipement de télécommunication (messages téléphoniques enregistrés, messages textes, etc.). Ces informations demeurent la propriété de la Commission et cette dernière se réserve le droit d'examiner, s'il y a lieu, l'ensemble des communications électroniques, écrites ou verbales (messages téléphoniques enregistrés), pour des motifs jugés raisonnables.

13.3 CONFIDENTIALITÉ DE L'INFORMATION

L'information contenue dans les ressources informatiques de la Commission est confidentielle si elle a le caractère d'un renseignement nominatif ou d'un renseignement que la Commission peut ou doit protéger en vertu d'une loi, d'un règlement, d'un contrat ou d'une entente de confidentialité.

Personne ne doit, à des fins autres que pour la réalisation des activités de la Commission, divulguer ou utiliser une information considérée comme confidentielle par la Commission. La divulgation de l'information doit alors être faite conformément aux lois, règlements ou politiques en vigueur.

La Commission ne peut garantir la confidentialité de toutes les communications se retrouvant sur les ressources informatiques de la Commission. L'utilisateur doit présumer que toute communication qu'il crée, envoie, reçoit ou archive sur les systèmes électroniques de la Commission peut être lue et entendue par quelqu'un d'autre que le destinataire.

13.4 ADRESSE ÉLECTRONIQUE

La Commission peut attribuer une adresse électronique aux membres du personnel ainsi qu'aux élèves. Comme toute autre ressource informatique de la Commission, cette adresse demeure la propriété de celle-ci et son utilisation doit être faite dans le respect des modalités d'application pour l'utilisation du courrier électronique.

Lorsqu'une adresse électronique a été attribuée à un membre du personnel, celui-ci se doit de l'utiliser dans le cadre de ses fonctions.

Lorsqu'un membre du personnel quitte la Commission, cette dernière se réserve le droit de conserver l'adresse électronique de celui-ci pendant 30 jours suivant son départ afin de s'assurer que des communications importantes puissent être transmises à la Commission**.** Celui-ci, après

entente avec la direction du Service des ressources informatiques, pourra consulter ses courriels pendant le même délai.

14. ENCADREMENT DE L'UTILISATION D'INTERNET

La multitude de renseignements et d'informations contenus sur les différents sites internet rend son accès de plus en plus populaire et la Commission doit s'assurer que l'usage qui en est fait est conforme à sa mission éducative et à ses fonctions administratives.

14.1 FILTRAGE

Le Service des ressources informatiques mettra en place des mécanismes de surveillance appropriés afin de s'assurer que l'usage qui est fait d'internet est conforme à la présente politique et aux modalités d'application.

À cet effet, le Service des ressources informatiques mettra en place des mécanismes de filtrage afin de limiter l'accès à certains sites internet, dont notamment les sites contenant du matériel pornographique, de la pédophilie, des propos racistes, obscènes ou vulgaires, des sites destinés aux jeux ou des sites contenant de la publicité interdite aux élèves de moins de 13 ans. Également, un contrôle pourra être exercé concernant la participation à des sites de clavardage, des forums de discussion et certains réseaux sociaux.

14.2 SURVEILLANCE DES ÉLÈVES

La direction d'établissement doit s'assurer qu'une surveillance adéquate est exercée à l'endroit des élèves qui utilisent internet afin d'éviter que ces derniers accèdent à des sites ou à des forums de discussion qui contreviennent à la présente politique.

La direction d'établissement est responsable de mettre en place des balises concernant l'utilisation d'internet par les élèves, l'utilisation du courrier électronique, de même que la participation des élèves à des forums de discussion ou à des services de clavardage. Ces balises doivent permettre notamment de sensibiliser les élèves à l'utilisation des renseignements personnels sur internet.

La direction ainsi que le personnel doivent être vigilants quant à l'usage que font les élèves du courrier électronique afin d'éviter notamment qu'ils tiennent des propos haineux ou malveillants à l'égard d'autres personnes ou encore que des messages malveillants leur soient acheminés. À cet égard, la direction doit informer les élèves qu'elle peut en tout temps consulter les messages électroniques qu'ils envoient ou qu'ils reçoivent dans le cadre d'activités scolaires comme elle peut le faire pour tous les travaux scolaires.

14.3 PROTECTION DES RENSEIGNEMENTS PERSONNELS

Avant de transmettre ou de diffuser des informations personnelles au sujet de ses employés, la direction de l'école, du centre ou du service doit s'assurer d'obtenir leur consentement écrit.

Le consentement écrit de l'élève majeur ou du titulaire de l'autorité parentale est nécessaire avant de transmettre ou de diffuser des informations personnelles, dont notamment des travaux scolaires.

15. UTILISATION DE LOGICIELS

La direction du Service des ressources informatiques ou son délégué est responsable de gérer l'acquisition, l'installation, la désinstallation et l'utilisation des logiciels. Elle est également responsable de la gestion des licences informatiques conformément à la *Loi sur le droit d'auteur.*

Toute installation ou utilisation de logiciels sans licence est interdite. Il est également interdit d'installer un logiciel sur un nombre de postes plus élevé que le nombre de licences détenues par l'établissement ou par la Commission.

La reproduction de logiciels n'est autorisée qu'à des fins de copies de sauvegarde ou selon les normes de la licence d'utilisation les régissant.

Il est interdit d'installer et d'utiliser un logiciel acquis pour un usage externe à la Commission sans que la licence ou le droit de propriété n'ait été transféré au nom de celle-ci.

16. VÉRIFICATION DE L'UTILISATION

Des vérifications sont occasionnellement effectuées par la direction du Service des ressources informatiques ou par un employé de son service à qui il donne le mandat, à la suite de demandes formulées afin de s'assurer du maintien d'un niveau de sécurité élevé et d'une utilisation appropriée des ressources informatiques.

Une vérification ponctuelle des informations personnelles d'un utilisateur, de son historique d'utilisation d'internet ou de son utilisation des ressources informatiques peut être effectuée, sans le consentement de ce dernier, si la Commission a des motifs raisonnables de croire que l'utilisateur fait usage des ressources informatiques en contravention à la présente politique, aux modalités d'application, aux lois ou aux règlements. La vérification est alors faite par la direction du Service des ressources informatiques ou par un employé de son service à qui il donne le mandat.

Au terme de l'opération de vérification, la direction du Service des ressources informatiques fait rapport aux autorités concernées et recommande, le cas échéant, les suites à donner.

La Commission se réserve le droit d'augmenter la fréquence de la surveillance de l'utilisation des ressources informatiques et de maintenir une surveillance constante d'un utilisateur lorsqu'elle a des raisons de le faire.

La direction du Service des ressources informatiques doit alors s'assurer de respecter les dispositions des lois visant la protection des renseignements personnels ainsi que la « Politique de gestion des documents » lorsqu'elle recueille, conserve, utilise ou communique certaines informations dans le cadre du contrôle et de la surveillance des ressources informatiques.

En cas d'urgence ou lors de l'absence d'un membre du personnel, la direction du Service des ressources informatiques peut accéder à ses ressources informatiques, récupérer ses données et en lire le contenu afin d'assurer le bon fonctionnement de la Commission.

17. SANCTIONS

Tout contrevenant à la présente politique et aux modalités d'application qui en découlent est passible, en plus des pénalités prévues à la loi, des sanctions suivantes :

- annulation ou suspension des droits d'accès aux équipements et services visés par la présente politique;
- remboursement à la Commission de toute somme que cette dernière serait dans l'obligation de défrayer suite à une utilisation illégale de ses ressources informatiques ou non conforme à la présente politique;
- pour le personnel, mesures disciplinaires pouvant aller jusqu'au congédiement et à des poursuites judiciaires imposées conformément aux conventions collectives et aux règlements de conditions d'emploi;
- pour les élèves, sanctions prévues dans le code de vie de l'école ou dans les règles de fonctionnement du centre.

18. MODIFICATION

La présente politique sera périodiquement évaluée afin de s'ajuster aux nouvelles pratiques et technologies utilisées à la Commission.

Toute modification à la présente politique doit être sanctionnée par le Conseil des commissaires de la Commission.