Conseil scolaire de district catholique des Aurores boréales.ca

DIRECTIVE ADMINISTRATIVE

E-001-D-2 UTILISATION ET SURVEILLANCE DES RESSOURCES INFORMATIQUES ET DES RÉSEAUX DE COMMUNICATION - PERSONNEL

Date d'approbation : le 9 décembre 2009
Date de révision : le 24 juin 2023

L'usage du masculin a pour but d'alléger le texte

1.0 DÉFINITIONS

Les définitions suivantes s'appliquent à la présente directive administrative :

Ressources informatiques : Sans limiter la généralité de cette expression, tous les serveurs physiques ou virtuels, les ordinateurs, les postes de travail informatisés, les tablettes, les téléphones intelligents et autres appareils informatiques similaires, de même que leurs unités ou accessoires périphériques de lecture, d'emmagasinage, 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, sur un média informatique ou dans un espace infonuagique, système de courrier électronique, système de messagerie vocale ou sur un site Web ou intranet , et tout réseau interne ou externe (incluant l'accès à l'Internet) de communication informatique dont le Conseil est propriétaire ou locataire, qu'il contrôle ou administre ou sur lesquels il possède un droit d'utilisation.

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

Droit d'auteur : Signifie tous les droits conférés par la common law ou 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. Accomplir ces actes sans le consentement du titulaire du droit constitue une violation du droit d'auteur.

Oeuvre : Signifie 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, vidéo, model 3D) ou sur un support informatique (cédérom, logiciel, disque dur, clé de mémoire flash) ou espace de stockage nuagique sur l'Internet.

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 la *loi sur la gestion de l'information et de la vie privée*.

2.0 OBJECTIFS

La présente directive administrative établit les conditions d'utilisation des ressources informatiques par les utilisateurs et vise à :

- promouvoir une utilisation responsable des ressources informatiques, conformément aux lois applicables;
- sensibiliser tous les utilisateurs sur leurs responsabilités en vertu de l'utilisation des ressources informatiques et des réseaux de communication.
- contribuer à la réalisation de la mission, de la vision et des objectifs stratégiques du Conseil;
- préserver la réputation du Conseil en tant qu'institution scolaire et communautaire à caractère francophone et à vocation catholique;
- prévenir une utilisation abusive ou illégale des ressources informatiques de la part des utilisateurs;
- assurer la protection des renseignements personnels;
- délimiter la sphère privée touchant la vie privée des utilisateurs dans leur utilisation des ressources informatiques;
- protéger la sécurité et l'intégrité des ressources informatiques, notamment en minimisant les risques de destruction ou de modification des systèmes et des données.
- renseigner les utilisateurs sur la surveillance électronique et les éventuelles sanctions applicables en cas d'utilisation inappropriée des ressources informatiques.
- prévenir les utilisateurs que la surveillance électronique peut avoir lieu à tout moment, sans autre préavis, pendant les heures de travail et autrement en relation avec les activités de travail, l'utilisation des ressources du Conseil, ou l'utilisation ou l'application des médias du CSDCAB;

- protéger l'intégrité de l'infrastructure électronique du Conseil (comme ses réseaux, serveurs, bases de données) et de l'équipement (comme les ordinateurs, tablettes électroniques et les téléphones intelligents) ;
- prévenir ou répondre à une inconduite, c'est-à-dire la violation des politiques et des attentes du Conseil ainsi que de toute loi applicable.

3.0 CONSIDÉRATIONS GÉNÉRALES

3.1 Privilège

L'accès aux ressources informatiques constitue un privilège et non pas un droit. Seuls les utilisateurs dûment autorisés peuvent avoir accès aux ressources informatiques et les utiliser dans les limites de l'autorisation accordée à l'utilisateur par le Conseil et conformément aux politiques et directives administratives pertinentes. L'utilisateur ne peut permettre qu'un tiers non autorisé utilise ces ressources.

3.2 Utilisation et surveillance des ressources informatiques

Les ressources informatiques sont mises à la disposition des utilisateurs pour la réalisation d'activités d'enseignement, d'apprentissage, de gestion, d'administration et de services à la communauté scolaire reliés à la réalisation de la mission et de la vision du Conseil et de ses établissements, et ce, dans l'exercice des fonctions de chacun des utilisateurs. Les utilisateurs doivent savoir que le Conseil 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.

3.3 Modification ou destruction

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

3.4 Actes préjudiciables

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 logiciels malveillants, 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 utilisateur, ou par des gestes visant à désactiver, défier ou contourner n'importe quel système de sécurité du Conseil.

3.5 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'utilisateur.

3.6 Utilisation convenable

Dans un contexte de partage équitable des ressources, l'utilisateur ne doit pas monopoliser ou abuser des ressources informatiques, entre autres, en effectuant un stockage abusif d'information ou en utilisant l'internet pour télécharger des fichiers de grand volume, des jeux vidéo ou des objets qui demandent une portion considérable de la bande passante. Le Conseil se réserve le droit de restreindre la bande passante de certains logiciels et d'assurer que les ressources sont adéquates pour l'enseignement ou des fins administratives.

3.7 Partage d'information numérique

L'utilisateur ne partagera pas des informations confidentielles ou sensibles par courriel ou par autre fin insécure. Le partage doit être verrouillé par des accès directs au destinataire, soit par l'entremise d'un service infonuagique comme OneDrive, GDrive ou tout autre service jugé sécure par le Conseil. Le partage d'information au public revient au Service des communications et ne sera jamais partagé par autre utilisateur du Conseil. Le Conseil pourrait bloquer ou retirer certaines informations partagées sans en aviser l'utilisateur, soit par des fins automatisées ou des interventions manuelles.

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.

N'étant pas une liste exhaustive, 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 du 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 l'Internet, 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 Internet, afficher l'œuvre artistique d'un tiers, et ce, lorsque ces œuvres sont protégées par le droit d'auteur.

4.2 Copie 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 (voir licence CanCopy).

5.0 COURRIER ÉLECTRONIQUE

5.1 Identification

Pour tout message électronique diffusé sur le réseau du Conseil, 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.

6.0 CONFIDENTIALITÉ ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

6.1 Renseignements confidentiels

Respect des mécanismes de protection

L'utilisateur doit respecter les règles édictées par la Loi sur l'accès à l'information municipale et la protection de la vie privée quant à la conservation, l'accès, la transmission et la diffusion des renseignements personnels, et ce, au moyen de ses ressources informatiques.

Diffusion de renseignements personnels

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

Lorsque l'utilisateur est un élève, il doit être informé, par le membre du personnel pertinent, des comportements à adopter dans la transmission de renseignements personnels le concernant ou concernant des membres de sa famille, des amis, d'autres élèves ou toute autre personne. En cas de doute, l'utilisateur devrait communiquer avec la direction de l'école.

6.2 Droit d'un utilisateur à la confidentialité et droit de surveillance et d'enquête du Conseil

Le Conseil respecte la vie privée des utilisateurs. Toutefois, les ressources informatiques du Conseil sont mises à la disposition des utilisateurs pour contribuer à la réalisation de sa mission, vision et objectifs stratégiques. Par conséquent, le droit à la vie privée de l'utilisateur est limité.

Le Conseil ne contrôle pas systématiquement les communications des utilisateurs ou la transmission d'informations des utilisateurs. Cependant, toute information ou

tout message qui est créé, envoyé, reçu, mémorisé ou auquel il est possible d'accéder par le biais des ressources informatiques du Conseil, y compris des réseaux de communication, sont la propriété du Conseil. Les ressources informatiques du Conseil sont accessibles en tout temps par le personnel du Service informatique. En outre, le Conseil effectue des vérifications périodiques concernant l'utilisation de ses ressources informatiques afin d'en assurer l'entretien, d'effectuer des réparations et d'en protéger l'intégrité, et ce, sans préavis. De plus, le Conseil peut effectuer des enquêtes, tel que précisé sous la rubrique 9.1 ci-dessous, également sans préavis.

Les utilisateurs doivent savoir que le Conseil 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. Dans la mesure où les utilisateurs se servent de mots de passe ou de codes d'usagers afin d'accéder à certaines ressources informatiques du Conseil, ceux-ci visent à protéger les ressources informatiques du Conseil et non à protéger la vie privée des utilisateurs. Le Conseil note que même si un message électronique a été effacé, une copie de sécurité peut exister et il peut être possible de reconstituer le message. De la même manière, les utilisateurs doivent savoir que certaines informations analogues à du métadonnées existent et peuvent être accessibles même si elles ne sont pas nécessairement visibles pour l'utilisateur.

L'utilisateur doit aussi savoir que le Conseil peut aussi être appelé, dans le cadre d'une procédure judiciaire ou quasi-judiciaire (y compris un arbitrage), à produire des preuves des informations enregistrées sur des supports informatiques qu'il détient. Dans un tel cas, le Conseil se réserve le droit et la possibilité d'entrer dans n'importe quel système sans préavis, et d'inspecter et de contrôler toutes données pertinentes.

L'utilisateur ne peut s'attendre à ce que le principe de vie privée soit respecté concernant toute information créée, envoyée, reçue ou mémorisée à partir des ressources informatiques du Conseil lorsqu'il utilise les ressources informatiques en contravention (i) à la présente directive administrative, (ii) à des ententes ou protocoles pertinents, ou (iii) aux lois et règlements provinciaux ou fédéraux.

7.0 RESPONSABILITÉS DU CONSEIL

7.1 Pertes dommages ou inconvénients

Le Conseil 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, 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.

8.0 UTILISATION INAPPROPRIÉE DES RESSOURCES INFORMATIQUES

8.1 Généralités

Toute utilisation des ressources informatiques du Conseil à des fins non autorisées ou illégales est strictement interdite. Sans limitée la portée générale de ce qui précède, et à titre d'illustration uniquement, il est interdit :

- 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, 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 et la vision éducative du Conseil;
- d'utiliser les ressources informatiques à des fins de propagande, de diffamation, de harcèlement ou de menace sous quelque forme que ce soit, ou pour jouer un tour à des tiers;
- d'utiliser des ressources informatiques personnelles (abonnements, logiciels) ou enfreindre les conditions d'utilisation d'une ressource informatique;
- d'utiliser les ressources informatiques pour transmettre de la publicité, faire la promotion ou effectuer des transactions dans le cadre d'un commerce personnel ou pour distribuer des pourriels;
- de participer à des jeux d'argent et de paris, de quelque nature que ce soit;
- de participer à des activités de piratage ou pouvant raisonnablement être soupçonnées de piratage (de musique, jeux, logiciels, etc.), et d'intrusion, de blocage ou d'engorgement 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, du Conseil ou de ses écoles;
- d'associer des propos personnels au nom du Conseil ou à celui d'une de ses écoles dans des groupes de discussion, des séances de clavardage, ou d'utiliser tout autre mode d'échanges d'opinions de manière à laisser croire que les opinions qui y sont exprimées sont endossées par le Conseil, 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.
- d'utiliser un ou des subterfuges ou d'autres moyens pour transmettre un courriel 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'introduire un logiciel malveillant dans les ressources informatiques du Conseil ou de toute personne physique ou morale;
- de désactiver, endommager, détruire ou enfreindre, de quelque façon que ce soit, toute mesure de sécurité mise en place afin de protéger l'intégrité des ressources informatiques du Conseil ou la confidentialité ou la sécurité d'un utilisateur;
- obtenir l'accès non autorisé (accéder, intercepter, surveiller ou sauvegarder) à des ressources, des données ou des communications pour laquelle l'utilisateur n'est pas approuvé ou destiné;
- d'expédier, sans autorisation, à tout le personnel ou à des groupes de membres du personnel, des messages sur des sujets d'intérêt divers ou à caractère personnel, des nouvelles de toutes sortes, des lettres en chaîne et toute information non pertinente aux activités du Conseil.

Aucune politique ou directive administrative ne peut prévoir de règles pour couvrir toutes les situations possibles. La présente vise à exprimer la philosophie du Conseil et à exposer des principes généraux en matière d'utilisation de ressources informatiques.

Le Conseil s'attend à ce que ses utilisateurs reconnaissent l'esprit et l'intention qui sous-tendent la présente directive administrative et qu'ils comprennent les objectifs qu'elle vise. Un utilisateur ne doit pas tenter d'accomplir indirectement ce que la présente directive administrative interdit directement. Un utilisateur ne doit pas non plus prendre des moyens pour contourner les objectifs de la présente directive administrative, même si ces moyens ne sont pas précisés par celle-ci.

Sous réserve des conventions collectives, conditions de travail pour le personnel non-syndiqué ou politiques pertinentes, tout employé utilisant de façon inappropriée les outils de communication appartenant au Conseil peut faire l'objet de mesures disciplinaires pouvant aller jusqu'au congédiement, et court le risque d'être poursuivi en justice ou d'être tenu responsable en droit criminel, selon le cas.

8.2 Procédures en cas de certaines infractions

8.2.1 Envoi ou réception de matériel à caractère extrême

Sont considérés comme du matériel inapproprié :

- La pornographie
- Tout matériel qui fait la promotion d'une violence extrême envers autrui
- Tout matériel présentant des êtres humains dans des activités à caractère sexuel

L'envoi de matériel de cette nature résultera automatiquement en une suspension, avec ou sans traitement lors de la période d'enquête.

Le fait d'accéder à de la pornographie juvénile à partir d'Internet résultera automatiquement en une suspension sans traitement, et ce, dès la première infraction lors de la période d'enquête.

Si les fichiers comportent de la pornographie infantile ou du matériel violent, un signalement doit être fait par l'autorité compétente aux services policiers.

8.2.2 Envoi ou réception de matériel offensant

Sont considérés comme du matériel offensant :

- Tout matériel montrant des corps dénudés d'hommes, de femmes ou d'enfants
- Tout matériel contribuant à créer un environnement de travail hostile (c.-à-d. du matériel relié au sexe, à la race, à l'âge, à la couleur de la peau, à l'origine ethnique, aux origines ancestrales, à la citoyenneté, à la religion, à un handicap, à l'orientation sexuelle ou à l'état civil).

  Le fait d'envoyer ou d'accéder à du matériel offensant déclenchera des mesures disciplinaires selon les étapes prévues dans la politique portant sur les mesures disciplinaires.

8.2.3 Réception ou connaissance de la réception de matériel offensant

- La réception par un employé ou le fait que cet employé ait connaissance qu'il y a eu réception de matériel offensant et ne prenne pas les mesures appropriées pourrait entraîner des mesures disciplinaires.

  Si un membre du personnel occupant un poste cadre reçoit lui-même du matériel extrême ou offensant d'un autre membre du personnel ou d'un contractuel, ou a connaissance qu'un membre du personnel ou un contractuel envoient du matériel de cette nature, l'expéditeur de ce matériel fera l'objet de mesures disciplinaires.

  De même, un membre du personnel occupant un poste cadre doit signaler au Service des ressources humaines toute infraction à cette politique et directive

administrative qui a, par la suite, la responsabilité d'assurer les suivis nécessaires.

Si l'employé occupant un poste cadre néglige de signaler les comportements décrits ci-dessus, il pourrait faire l'objet de mesures disciplinaires.

- L'employé n'occupant pas un poste cadre qui reçoit du matériel inapproprié fera l'objet d'un rappel de la politique.

Les membres du personnel n'occupant pas un poste cadre et qui reçoivent du matériel extrême ou offensant reçoivent un avis écrit concernant les attentes du Conseil à cet égard. Ce rappel inclura des suggestions en vue de décourager l'envoi d'un tel matériel à l'avenir, et proposera aussi à la personne concernée des actions à mettre en pratique.

Les actions proposées pourraient inclure :

- Envoyer une réponse directe à l'expéditeur (si celui-ci est un autre employé ou un contractuel, ou si l'expéditeur est une personne qui n'est pas un employé du Conseil, mais est une personne connue du destinataire du message), lui précisant de cesser d'envoyer de tels messages.
- Communiquer avec le Service informatique afin de mettre en place des règles de gestion des courriels qui permettront de détruire automatiquement les courriels possédant certaines caractéristiques bien définies, telles que certains mots ou termes dans le champ « objet » ou l'adresse d'un expéditeur en particulier.
- Rappeler à tout employé qui envoie du matériel de ce genre qu'il commet une infraction aux politiques et aux attentes du Conseil et que ces pratiques doivent cesser.
- À la discrétion de l'employé, faire appel à son superviseur ou au Service des ressources humaines afin d'obtenir de l'aide ou des conseils.

Le fait de ne pas se conformer aux directives ci-dessus pourra entraîner des mesures disciplinaires à l'encontre des employés concernés.

NOTE : Tous les employés doivent dissuader toute personne extérieure au Conseil de leur envoyer du matériel inapproprié.

9.0 SURVEILLANCE, VÉRIFICATIONS, ENQUÊTES ET MESURES DE SÉCURITÉ

9.1 Vérifications et enquêtes

Le Conseil se réserve le droit de tenir un registre des transactions effectuées avec ses ressources informatiques (y compris concernant les systèmes de cartes d'accès et de caméras de surveillance dans les lieux de travail, les sites Web

auxquels les utilisateurs ont accédé et les heures auxquelles ceux-ci ont été accédés) et ses réseaux de communication et celui d'analyser l'information contenue dans ce registre afin d'assurer l'entretien, la réparation, la gestion et l'intégrité de ses ressources informatiques de même que pour détecter les activités non autorisées, illicites ou illégales sur son réseau.

Le Conseil a ainsi le droit d'accéder, de surveiller, de récupérer et de lire toute communication (y compris des courriels) ou donnée électronique créée, envoyée reçue ou mémorisée à partir de ressources informatiques du Conseil (y compris ses systèmes de cartes d'accès et de caméras de surveillance), sans préavis, aux fins suivantes :

- Assurer la santé et la sécurité du milieu scolaire, y compris des élèves et des membres du personnel;
- Assurer l'entretien et la réparation ainsi que protéger la sécurité et l'intégrité des ressources informatiques du Conseil;
- Protéger les intérêts du Conseil en cas de responsabilité civile, y compris pour la diffamation ou la violation de droits d'auteurs;
- Prévenir l'usage inapproprié d'informations appartenant à ou recueilli par le Conseil, y compris des informations confidentielles au sujet d'élèves;
- Prévenir les activités illégales, malhonnêtes ou l'inconduite d'employés ou d'élèves;
- Vérifier les activités d'un membre du personnel;
- Protéger la réputation du Conseil comme institution pédagogique, à caractère catholique;
- Rencontrer ses obligations en vertu de la *Loi sur l'éducation*, la *Loi sur la santé et sécurité au travail* et toute autre loi pertinente;
- Assurer le respect de conventions collectives en vigueur, de la présente directive administrative et de toute autre politique ou directive administrative du Conseil, y compris en matière de ressources humaines.

Le Conseil se réserve le droit de mener une enquête et de faire les suivis qui s'imposent aux fins susmentionnées, y compris de communiquer avec ou de divulguer des informations à toute autorité officielle, organisation ou tierce partie intéressée, lorsqu'appropriée, notamment à la Société de l'aide à l'enfance et aux services policiers. Dans cette optique, le Conseil est autorisé, en tout temps et sans préavis, à surveiller, enregistrer, recueillir, et conserver toutes copies de documents, données ou informations. Une telle enquête peut être menée dès lors que le Conseil a des motifs raisonnables de croire que les ressources informatiques sont utilisées de manière inappropriée ou pour l'une des fins susmentionnées, que ce soit à la suite de vérifications périodiques concernant l'utilisation de ses

ressources informatiques ou autrement. Pour être clair, ce type d'enquête peut comprendre la surveillance, l'enregistrement ou la cueillette et conservation de données et d'informations tirés des ressources informatiques du Conseil de même que ses systèmes de carte d'accès et de surveillance vidéo. La direction de l'éducation ou sa personne déléguée est responsable des enquêtes découlant de la présente politique.

Le Conseil se réserve le droit de supprimer ou de bloquer tout contenu illégal ou qui contrevient aux dispositions de la présente politique et directive administrative ou de restreindre autrement l'accès aux ressources informatiques.

9.2 Suspension des droits d'accès pendant une vérification

Les droits d'accès d'un utilisateur peuvent être suspendus pendant la durée d'une vérification. Une telle décision incombe à la direction exécutive du Service des ressources humaines en consultation avec le supérieur immédiat de la personne.

9.3 Sécurité

Le Service informatique met en place les outils informatiques assurant :

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

Le Service informatique a la responsabilité d'émettre des directives et règlements pour assurer la sécurité des ressources informatiques et procéder périodiquement à des vérifications de sécurité.

Le Service informatique se réserve le droit de bloquer, à sa discrétion, l'accès à certaines des ressources informatiques ainsi qu'à certains sites Web.

9.4 Surveillance

Au-delà des contextes de vérifications et d'enquêtes actives mentionnées au paragraphe 9.1 ci-dessus, tous les membres du personnel du Conseil doivent savoir que la plupart des activités de surveillance électronique sont de nature passive, c'est-à-dire qu'elles s'effectuent automatiquement par l'entremise de systèmes pare-feu ou d'enregistrement de données ou de communication, ou encore via les systèmes de carte d'accès et de surveillance vidéo, par exemple. Toutefois, tel que précisé ci-dessus, le Conseil peut s'engager dans de la surveillance active pour les fins précisées au paragraphe 9.1.

La surveillance électronique peut avoir lieu à tout moment lorsqu'il s'agit de l'utilisation des ressources informatiques du Conseil et autrement sur les lieux de travail par l'entremise des systèmes de carte d'accès et de surveillance vidéo.

Les documents, données ou informations ainsi recueillies peuvent être utilisés :

- dans le cadre d'instances judiciaires impliquant le Conseil (y compris devant des arbitres ou des tribunaux;
- dans le but d'assurer le respect des politiques, et des directives administratives du Conseil de même que des lois pertinentes;
- pour protéger l'infrastructure électronique et les ressources électroniques du Conseil;
- pour vérifier tout abus potentiel des ressources du Conseil (y compris le vol de temps);
- afin d'assurer la continuité des opérations du Conseil (en outre, lors du départ ou de l'absence d'un membre du personnel);
- pour prévenir ou répondre aux inconduites liées au travail, y compris à des fins de coaching ou de discipline; et
- d'assurer le bien-être, la santé et la sécurité des membres de la communauté scolaire, y compris les élèves et les personnes ayant accès aux établissements du Conseil.

10.0 COLLABORATION

Tout membre du personnel devra prendre connaissance de la directive administrative sur l'utilisation et surveillance des ressources informatiques et des réseaux de communication.

L'utilisateur collabore avec le Service informatique afin de faciliter l'identification et la correction des problèmes ou anomalies pouvant se présenter concernant les équipements et les ressources informatiques du Conseil.