

P-24 | Politique relative à la sécurité de l'information et à l'utilisation des ressources informatiques et des médias sociaux

Table des matières

1.	CONTEXTE	3
2.	OBJECTIFS.....	3
3.	CHAMP D'APPLICATION.....	4
4.	CADRE LÉGAL	4
5.	DÉFINITIONS	5
6.	RÔLES ET RESPONSABILITÉS	7
6.1	Centre de services scolaire des Hauts-Cantons.....	7
6.2	Service des technologies de l'information (STI).....	7
6.3	Chef de la sécurité de l'information organisationnelle (CSIO)	7
6.4	Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI).....	8
6.5	Comité sur l'accès à l'information et la protection des renseignements personnels	8
6.6	Service des ressources matérielles	8
6.7	Services des archives	8
6.8	Service des ressources humaines	8
6.9	Directions d'établissement et de service.....	9
6.10	Utilisateur	9
7.	SÉCURITÉ DE L'INFORMATION	10
7.1	Principes généraux.....	10
7.2	Accès aux actifs informationnels.....	10
7.3	Gestion des actifs informationnels	10
7.4	Sauvegarde de données.....	10
7.5	Travail à distance.....	11
7.6	Ententes et contrats	11
7.7	Vérification par le CSSHC	11
7.7.1	Droit de regard	11
7.7.2	Filtrage.....	12
7.8	Exercice annuel de sensibilisation	12

Adoptée le : 2 décembre 2025	Unité responsable : Service de l'informatique
Dernier amendement le : 2 décembre 2025	Numéro de résolution : CA25-562

8.	UTILISATION DES RESSOURCES INFORMATIQUES	13
8.1	Principes généraux	13
8.1.1	Privilège	13
8.1.2	Conditions d'utilisation	13
8.1.3	Usage à des fins professionnelles	13
8.1.4	Usage à des fins personnelles	14
8.1.5	Limite à la vie privée des utilisateurs	14
8.1.6	Pertes, dommages et inconvénients	14
8.1.7	Accès non autorisé	15
8.1.8	Utilisation de la langue française	15
8.2	Droit d'auteur et propriété intellectuelle	15
8.2.1	Utilisation	15
8.2.2	Création	15
8.3	Outils de travail et de communication	16
8.3.1	Courrier électronique	16
8.3.2	Téléphone de bureau et boîte vocale	17
8.3.3	Téléphone cellulaire	17
8.3.4	Ordinateur portable et tablette	18
8.3.5	Mozaïk- Portail	18
8.3.6	Sites Web	19
8.4	Confidentialité et protection des renseignements	19
8.4.1	Renseignements confidentiels	19
9.	UTILISATION DES MÉDIAS SOCIAUX	20
9.1	Principes généraux	20
9.1.1	Faire preuve de jugement, de discernement et de civilité	20
9.1.2	Le droit de ne pas voir son identité usurpée	20
9.1.3	Le droit de ne pas voir diffuser des images de soi (photo ou vidéo) sans son consentement	20
9.2	Principes applicables aux membres du personnel	21
9.2.1	Le rôle de modèle face aux élèves, pendant et en dehors des heures de travail	21
9.2.2	L'obligation générale de civilité envers les collègues, les élèves et les parents	21
9.2.3	L'obligation de l'employeur de protéger ses employés contre le harcèlement psychologique	21
10.	UTILISATION DE L'INTELLIGENCE ARTIFICIELLE	22
11.	SANCTIONS	22
12.	ENTRÉE EN VIGUEUR	23

1. CONTEXTE

Le Centre de services scolaire des Hauts-Cantons (le « CSSHC ») reconnaît l'importance de fournir à son personnel ainsi qu'à ses élèves et leurs parents un accès à ses ressources informatiques et de télécommunication afin de soutenir le travail scolaire, pédagogique et administratif de ceux-ci.

Compte tenu de la nature hautement sensible des renseignements qui peuvent être manipulés, tout utilisateur doit être informé des bonnes pratiques et de ses responsabilités en lien avec la sécurité de l'information, et s'assurer de les respecter.

Le CSSHC reconnaît également l'omniprésence des médias sociaux, qui font partie intégrante de la vie étudiante. Bien que ceux-ci créent de nombreux avantages au niveau des communications, des dommages considérables pourraient être causés en cas de mauvaise utilisation.

Dans le cadre de sa mission éducative, le CSSHC souhaite ainsi contribuer à ce que ses élèves développent une utilisation éthique, responsable et positive des médias sociaux, ainsi qu'une intégrité intellectuelle face à l'utilisation de l'intelligence artificielle générative. Ces démarches nécessitent que les membres de son personnel en soient tout autant sensibilisés et qu'ils agissent eux-mêmes de la sorte, et ce, en tout temps.

Pour soutenir son engagement à opérer un environnement numérique adéquat, sécuritaire et conforme à sa mission et à la législation en vigueur, le CSSHC vise par la présente politique à renforcer la gouvernance de la sécurité de l'information, de l'utilisation des ressources informatiques et des médias sociaux.

2. OBJECTIFS

La présente politique vise notamment à :

- Définir un cadre général régissant l'utilisation des ressources informatiques et des télécommunications du CSSHC, et des médias sociaux dans le respect de sa mission éducative, des exigences ministérielles en matière de confidentialité et de cybersécurité ainsi que des différentes lois et normes qui régissent ce secteur d'activités;
- Préciser les droits, devoirs et responsabilités de chaque acteur, incluant les utilisateurs;
- Sensibiliser et former les élèves et les membres du personnel au sujet des enjeux éthiques, professionnels et interpersonnels liés à l'utilisation des médias sociaux;
- Contribuer au développement de saines habitudes d'utilisation de l'intelligence artificielle chez les élèves et les membres du personnel et s'assurer qu'elle est utilisée de façon à optimiser les apprentissages;
- Définir des normes d'utilisation des ressources afin d'assurer la sécurité et l'intégrité des infrastructures informatiques, le bon fonctionnement des équipements, le respect du droit d'auteur, de la vie privée des usagers et de la protection des renseignements personnels détenus par le CSSHC;
- Sensibiliser les utilisateurs aux réalités et enjeux en matière de cybersécurité et de protection des renseignements personnels;
- Préserver la réputation du CSSHC comme organisme éducatif responsable.

3. CHAMP D'APPLICATION

La présente politique s'adresse à tous les utilisateurs de l'information, c'est-à-dire à tout le personnel, peu importe son statut, à toute personne physique ou morale qui à titre d'élève, de parent, de partenaire, de consultant, de fournisseur, ou de visiteur utilise les actifs informationnels du CSSHC ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

Elle s'applique dans le cadre des activités tant professionnelles que personnelles des utilisateurs, sans égard au lieu où se produisent ces activités, et couvre toutes les données recueillies, saisies, traitées ou enregistrées sur quelque support que ce soit appartenant au CSSHC.

4. CADRE LÉGAL

La politique s'appuie et s'interprète en conformité avec les différents règlements, encadrements et lois qui régissent ce type d'activités, notamment :

- *La Charte des droits et libertés de la personne* (LRQ, chapitre C-12);
- *Code civil du Québec* (LQ, 1991, chapitre 64);
- *La Loi sur l'instruction publique* (L.R.Q. c. I-13.3);
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03);
- *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1);
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1);
- *Code criminel* (LRC, 1985, chapitre C-46);
- *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42);
- *Loi sur les archives* (LRQ, A-21.1);
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, Loi 133)
- *La Directive sur la sécurité de l'information gouvernementale* (DSIG)
- Les mesures minimales en matière de cybersécurité par le ministère de la Cybersécurité et du Numérique;
- *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques* (L.R.Q. c. A-21.1, r.1);
- *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RRQ, chapitre A-2.1, r. 2);
- *L'utilisation pédagogique, éthique et légale de l'intelligence artificielle générative*, Guide produit par le Gouvernement.

5. DÉFINITIONS

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

Actif informationnel	Ce terme désigne tant l'information consignée dans un document que le système qui permet de la prendre en charge. L'actif informationnel peut être constitué de documents numériques ou de documents en format papier ou encore d'une banque de données. Il peut s'agir aussi d'une technologie de l'information, d'une installation, d'un bien informatique ou d'un ensemble de ces éléments.
Cycle de vie de l'information	Le cycle de vie de l'information consiste en l'ensemble des étapes que franchit une information depuis sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation du CSSHC.
Document	Ce terme désigne un ensemble constitué d'information qui se trouve sur un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support, et est intelligible sous forme de mots, de sons ou d'images. Elle peut être communiquée au moyen de quelque mode d'écriture que ce soit, y compris un système de symboles transcrits sous l'une de ces formes. Est assimilée à un document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.
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 quelqu'un d'autre 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.
Gestion des incidents	Le processus de la gestion des incidents permet de préparer l'organisation en vue de la prise en charge d'incidents susceptibles de compromettre la sécurité de l'information, depuis cette prise en charge jusqu'au retour à la normale. Il prévoit, le cas échéant, l'escalade jusqu'aux autorités ministérielles ou gouvernementales. Il prévoit également l'arrimage avec d'autres processus du CSSHC, dont le plan local des mesures d'urgence.
Intelligence artificielle générative (IAG)	Système informatique qui utilise des modèles d'intelligence artificielle probabilistes pour générer automatiquement des contenus variés (texte, image, voix, musique, vidéo, présentation, etc.) en réponse à une requête faite par une personne utilisatrice.

Médias 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 X); • les blogues, personnels ou corporatifs; • les forums de discussion (Yahoo!, Google groups, 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.
Nétiquette	Ensemble des conventions de bienséance régissant le comportement des internautes dans le réseau, lors des échanges, tant écrits que multimédias, notamment dans les forums, les blogues, en visioconférence, par textos, par courrier électronique ou en utilisant des médias sociaux. La nétiquette énonce les règles de politesse et de savoir-vivre dans l'utilisation des services sur le Web.
Œuvre	Signifie notamment toute œuvre littéraire, dramatique, musicale, visuelle ou artistique, une banque de données ou d'information (textuelle, sonore, symbolique ou visuelle), une 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, clé USB, carte mémoire) ou accessible par réseau
Ressources informatiques	Tout matériel pouvant contenir, afficher ou communiquer du contenu numérique, dont le CSSHC est propriétaire ou locataire, qu'il contrôle ou administre ou sur lequel il possède un droit d'utilisation.
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. Exemples : nom, adresse, numéro d'assurance sociale, date de naissance, numéro de téléphone, pièces d'identité, photos, etc.
Sécurité physique	La sécurité physique concerne la protection de l'accès physique à des lieux, à de l'équipement, à du matériel, à des documents et à des personnes.
Utilisateur	Membre du personnel, élève jeune ou adulte, parent d'élève ainsi que toute personne physique ou morale appelée ou autorisée à utiliser les ressources informatiques

6. RÔLES ET RESPONSABILITÉS

6.1 Centre de services scolaire des Hauts-Cantons

Le conseil d'administration adopte la présente politique et autorise les unités administratives du CSSHC à agir tel que le prévoit la politique, le tout, dans le respect du [Règlement de délégation de fonctions et de pouvoirs](#).

La Direction générale du CSSHC est la première responsable de la sécurité de l'information. À ce titre, elle veille au respect du cadre gouvernemental de sécurité de l'information et s'acquitte de ses obligations telles qu'elles sont édictées dans la [Directive sur la sécurité de l'information gouvernementale](#).

6.2 Service des technologies de l'information (STI)

Le Service des technologies de l'information est responsable de soutenir les établissements et services dans l'utilisation des équipements, des logiciels et des infrastructures de télécommunications, et ce tant sur le plan pédagogique qu'administratif.

Il est notamment chargé de l'élaboration et du maintien d'outils conformes aux objectifs gouvernementaux en matière de sécurité de l'information. Cela implique de mettre en œuvre des projets de développement ou d'acquisition des systèmes d'information, de participer aux analyses de risques, de veiller à anticiper les menaces à la sécurité des systèmes d'information, de prendre toutes les mesures nécessaires pour contrer les menaces ou tout incident en matière de sécurité de l'information, et de participer à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par la direction générale.

6.3 Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO est nommé par le conseil d'administration. Il relève du directeur général au sens du Cadre gouvernemental de gestion de la sécurité de l'information.

Ses principales responsabilités sont :

- Conseiller la haute direction sur les orientations stratégiques;
- Assurer la coordination et la cohérence des actions de la sécurité de l'information (SI) menées au sein du CSSHC par tous les intervenants;
- Communiquer et coordonner la mise en œuvre des processus;
- Voir à la reddition de compte avec le COMSI;
- Établir des liens avec les autres CSIO.

6.4 Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le COMSI, nommé par le conseil d'administration, apporte son soutien au CSIO, notamment en ce qui a trait à la gestion des incidents et des risques en sécurité de l'information.

Ses principales responsabilités sont :

- Mettre en œuvre les processus SI;
- Contribuer aux analyses des risques de la SI (ex. : exposition aux cyberattaques);
- Coordonner la gestion d'incidents à portée gouvernementale;
- Procéder à l'autoévaluation de la sécurité des systèmes informatiques du CSSHC;
- Maintenir une veille continue sur les risques, les menaces et les vulnérabilités;
- Maintenir un lien avec les autres COMSI.

6.5 Comité sur l'accès à l'information et la protection des renseignements personnels

Le Comité sur l'accès à l'information et la protection des renseignements personnels (le « Comité sur l'accès ») chargé de soutenir le CSSHC dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en lien avec la protection des renseignements personnels.

Il doit notamment être consulté et approuver les règles encadrant la gouvernance à l'égard des renseignements personnels, et être consulté à l'occasion d'une évaluation des facteurs relatifs à la vie privée d'un projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

6.6 Service des ressources matérielles

Le Service des ressources matérielles participe, avec le COMSI/CSIO, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du CSSHC. Il émet également des contrats aux partenaires qui offrent des prestations de service conformes à cette politique et à la réglementation applicable.

6.7 Services des archives

Le service des archives a pour mission de collecter, classer, conserver, communiquer et mettre en valeur l'ensemble des documents d'archives produits ou reçus. Pour cela, il effectue un tri et procède à l'élimination des archives qu'il gère conformément aux règles et aux termes des durées légales de conservation.

6.8 Service des ressources humaines

Le Service des ressources humaines, en collaboration avec le supérieur immédiat, s'assure que tout employé du CSSHC soit avisé de la présente politique et qu'il s'engage à la respecter en signant le formulaire prévu à cet effet. Également, il supporte la direction concernée lorsqu'un utilisateur contrevient aux dispositions de la politique.

6.9 Directions d'établissement et de service

En matière de sécurité de l'information, la direction voit à l'application de la politique et des directives qui en découleront. Elle est la détentrice de l'information. Son rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de cet établissement ou service. Plus précisément, elle :

- Prend connaissance de la présente politique et s'assure de sa diffusion dans son établissement ou service;
- Voit à la protection de l'information et des systèmes d'information sous sa responsabilité;
- Intervient auprès de son personnel lorsqu'elle constate une pratique qui peut compromettre la sécurité de l'information;
- Récupère tout matériel informatique assigné à un membre de son personnel lorsque celui-ci quitte, conformément au Guide de gestion des équipements informatiques centralisé;
- Collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information ainsi qu'à toute opération de vérification de la sécurité de l'actif informationnel;
- Signale au Service des technologies de l'information toute menace ou tout incident afférant à la sécurité de l'information, et tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'un membre du personnel.

6.10 Utilisateur

La responsabilité de la sécurité de l'information incombe à tous les utilisateurs des actifs informationnels du CSSHC. Tout utilisateur ayant des privilèges d'accès aux actifs informationnels a l'obligation de protéger l'information mise à sa disposition et est imputable de ses actions.

L'utilisateur a notamment les responsabilités suivantes :

- Conserver et s'abstenir de partager les accès qui lui sont attribués (clés, puces, mots de passe, etc.);
- Utiliser l'information, quel que soit le support sur lequel elle se trouve, avec discernement, aux seules fins auxquelles elle est destinée et exclusivement selon les droits qui lui sont accordés;
- S'abstenir d'utiliser des informations ou des accès privilégiés à des fins personnelles ou à des fins qui constitueraient un conflit d'intérêt ou de rôle;
- S'assurer de l'intégrité et de la confidentialité de l'information du CSSHC;
- Assurer, le moment venu, la destruction sécuritaire des documents sensibles;
- Utiliser uniquement l'équipement et les logiciels pour lesquels il est autorisé;
- Respecter les mesures de sécurité mises en place sur le poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier leur configuration ou les désactiver;
- Respecter les droits de propriété intellectuelle au moment de l'utilisation des produits et des documents;
- Agir avec précaution, notamment en s'abstenant d'utiliser l'information s'il a des doutes sur les règles applicables;
- Signaler sans tarder à la direction ou au Service des technologies de l'information (support@csshc.gouv.qc.ca ou composer le 3333) toute situation, incident, ou anomalie susceptible de compromettre la sécurité des actifs informationnels du CSSHC;
- Participer aux activités de sensibilisation et de formation qui sont offertes par le CSSHC;
- Remettre, au moment de son départ, les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie mis à sa disposition.

7. SÉCURITÉ DE L'INFORMATION

7.1 Principes généraux

Les principes qui guident les actions du CSSHC en matière de sécurité de l'information sont les suivants :

- a) Identifier l'information à protéger;
- b) Protéger le cycle de vie de l'information;
- c) Permettre que chaque employé ait accès uniquement aux renseignements qui sont requis pour accomplir ses tâches (caractère de nécessité);
- d) Sensibiliser et former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en la matière.

7.2 Accès aux actifs informationnels

Tout système d'information doit être protégé, au minimum, par un processus d'accès nécessitant un mécanisme d'identification et d'authentification de l'utilisateur permettant de retracer les activités de celui-ci.

L'accès aux actifs informationnels est limité aux seuls utilisateurs dont les tâches l'exigent dans l'exercice de leurs fonctions et qui détiennent en conséquence un privilège d'accès approprié.

7.3 Gestion des actifs informationnels

Le CSSHC maintient à jour un registre des actifs informationnels comprenant leur identification, leur catégorisation selon leur valeur et leur sensibilité, de même que la désignation de leur détenteur.

Le CSSHC met en place et fait une mise à jour régulière du plan de relève des actifs informationnels, du plan de sauvegarde et des registres de sécurité concernant les privilèges d'accès et les incidents de sécurité.

Tout projet de conception d'applications ou de mise en œuvre de projets d'informatisation doit tenir compte des obligations en matière de sécurité des actifs informationnels.

Le processus de destruction de l'information n'est engagé que lorsque les renseignements recueillis ne sont plus nécessaires et qu'il est autorisé d'en disposer de manière sécuritaire, selon les modalités d'application du calendrier de conservation du centre d'archives du CSSHC.

7.4 Sauvegarde de données

En cas de bris de matériel ou de défaillance logicielle, et ce, dans la mesure du possible, le CSSHC s'engage à restaurer le système dans l'état original de livraison (configuration initiale). Le maintien, la sauvegarde et la restauration de toute autre ressource logicielle (incluant les applications), ainsi que les données sont de la responsabilité de l'utilisateur.

Seules les données sauvegardées sur les espaces de stockage réseau ou infonuagique autorisés par le CSSHC peuvent être récupérées en cas de bris, de réinitialisation ou d'effacement volontaire. Toute sauvegarde effectuée sur un espace de stockage local ou externe non contrôlé par le CSSHC ne pourra être récupérée.

En aucun cas le CSSHC, le STI ou ses techniciens ne pourront être tenus responsables de bris de matériel, de pertes de données ou de frais engagés par l'utilisateur.

7.5 Travail à distance

Un utilisateur désirant effectuer du travail à distance doit prendre connaissance et respecter le [Cadre de référence en matière de télétravail](#).

De façon générale, il n'est pas permis d'apporter à l'extérieur des établissements du CSSHC tout document jugé confidentiel. Toutefois, lorsque cela est nécessaire pour assurer la continuité des opérations, un employé ayant obtenu l'autorisation de son supérieur immédiat peut le faire, sous réserve de respecter des règles de confidentialité ainsi que les balises édictées par son ordre professionnel, s'il y a lieu.

L'utilisation des logiciels administratifs du CSSHC est possible en utilisant un accès sécurisé et en ayant recours à une authentification rencontrant les normes de sécurité en vigueur.

Le STI offre des ressources numériques qui permettent au personnel du CSSHC de réaliser leur travail au Canada. Pour des motifs de sécurité, et à moins d'une autorisation spécifique de la direction générale, l'utilisation de ces outils n'est pas disponible à l'étranger.

Certaines permissions sont possibles pour des situations particulières ou pour réaliser un mandat précis à la demande de la direction générale.

7.6 Ententes et contrats

Les ententes et contrats du CSSHC avec tout autre établissement, organisme, ou fournisseur en lien avec les actifs informationnels doivent contenir les clauses appropriées pour garantir le respect de la présente politique et directives, normes et procédures qui en découlent.

Afin de répondre à l'obligation de protection des renseignements personnels, toute entente ou contrat par lequel un tiers est susceptible d'avoir accès à des actifs informationnels doit notamment justifier les raisons de son usage et préciser les moyens utilisés pour en assurer la confidentialité.

Avant de conclure un contrat portant sur un projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels, le CSSHC doit saisir son Comité sur l'accès afin que soit réalisée une évaluation des facteurs relatifs à la vie privée et dont les conclusions sont favorables.

Les ententes et contrats sont des documents essentiels et officiels. Par conséquent, ils doivent être acheminés et protégés au service des archives du CSSHC pour leur traitement et leur conservation (peu importe le support).

7.7 Vérification par le CSSHC

7.7.1 Droit de regard

Le CSSHC a un droit de regard sur l'emploi de ses actifs informationnels par les utilisateurs. De ce fait, toute expectative de l'utilisateur en matière de vie privée s'en trouve restreinte.

Le STI met en place les outils informatiques assurant :

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

Le STI peut également édicter des directives et règles pour assurer la sécurité des ressources informatiques, et procéder à des audits de sécurité.

Le CSSHC se réserve le droit de tenir un registre des transactions effectuées avec ses ressources informatiques et d'analyser les informations contenues dans ce registre afin de détecter les activités non autorisées, illicites ou

illégalles sur son réseau. Il peut également 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.

Les directions d'établissement et de service sont autorisées en tout temps et sans préavis à procéder à toutes les vérifications estimées nécessaires et à effectuer 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 CSSHC pour assurer l'application des ententes et protocoles pertinents du CSSHC ou des lois ou des règlements provinciaux ou fédéraux.

L'utilisateur doit savoir aussi que le CSSHC peut être appelé, dans le cadre d'une procédure judiciaire, à produire en preuve toute information emmagasinée sur ses supports informatiques. Dans un tel cas, le CSSHC se réserve le droit d'entrer dans n'importe quel système sans préavis, et d'inspecter et contrôler toutes les données qu'il contient.

7.7.2 Filtrage

Le STI met également 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. Des mécanismes de filtrage sont utilisés afin de limiter l'accès à certains sites Internet, notamment les sites contenant du matériel pornographique, de la pédophilie, des propos racistes, obscènes ou vulgaires ou des sites destinés aux jeux. Les mécanismes de surveillance n'étant toutefois pas infaillibles, la surveillance par le personnel continue d'être de mise.

Dans l'éventualité où un site bloqué serait nécessaire au travail d'un utilisateur, une demande de déblocage devra être faite à la direction du STI par la direction de l'utilisateur concerné.

D'autres mécanismes de contrôle sont installés afin d'analyser le trafic sur le réseau informatique du CSSHC. Ces mécanismes analysent notamment la présence de logiciels malveillants ainsi que les tentatives de vol d'information. Malgré ces contrôles, l'utilisateur doit rester vigilant en évitant de télécharger des pièces jointes ou de cliquer sur des liens dont il en ignore la provenance.

7.8 Exercice annuel de sensibilisation

Le ministère de la cybersécurité et du numérique (MCN) exige des organisations de former et sensibiliser de manière continue l'ensemble de leur personnel ainsi que leurs élèves sur les enjeux liés à la navigation sur Internet et sur les bonnes pratiques à adopter en matière de cybersécurité et de sécurité de l'information.

Le personnel doit donc participer annuellement à la campagne de sensibilisation en réalisant les activités prévues par le STI.

La direction déterminera un moment sur le temps de travail pendant lequel ces activités pourront être réalisées.

Un membre du personnel qui refuse de participer aux exercices demandés pourrait être soumis à des fonctions de sécurité supplémentaires, tel qu'une demande d'authentification rencontrant les normes de sécurité en vigueur à l'intérieur du réseau ou des restrictions d'accès à nos services à l'extérieur des murs.

Le STI verra également à offrir aux élèves des capsules de sensibilisation afin de les informer des enjeux de sécurité du moment.

8. UTILISATION DES RESSOURCES INFORMATIQUES

8.1 Principes généraux

8.1.1 Droit d'accès

L'accès aux ressources informatiques est accordé aux utilisateurs par le CSSHC. Il revient à chaque utilisateur de respecter la présente politique, à défaut de quoi le CSSHC se réserve le droit de restreindre des accès.

Seuls les utilisateurs dûment autorisés peuvent avoir accès aux ressources informatiques, et ce, dans les limites de l'autorisation accordée à l'usager par le CSSHC. L'usager ne peut permettre qu'un tiers non autorisé utilise ces ressources.

L'utilisation doit être raisonnable et ne pas avoir pour effet de limiter indûment l'accès aux ressources informatiques aux autres utilisateurs.

8.1.2 Conditions d'utilisation

Tout utilisateur doit :

- Toujours s'identifier lorsqu'il envoie 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 du CSSHC, de ses établissements, du personnel et des élèves;
- Avant d'utiliser un logiciel, une application ou tout autre service en ligne, s'assurer qu'il est autorisé et supporté par le Service des ressources informatiques et qu'il est accompagné d'une licence. Constitue un logiciel, une application ou un service en ligne autorisé celui dont les résultats de l'analyse de sécurité répondent aux normes gouvernementales en vigueur;
- S'assurer auprès du Service des ressources informatiques que tout téléchargement ne peut entraver l'intégrité du réseau ni le bon fonctionnement des ordinateurs, et;
- Respecter les mesures de sécurité, notamment et non limitativement, les filtres internet et les coupe-feux établis par le CSSHC.

8.1.3 Usage à des fins professionnelles

Les ressources informatiques sont mises à la disposition des utilisateurs pour la réalisation d'activités d'enseignement (incluant la préparation d'activités pédagogiques), d'apprentissage, de développement professionnel, de gestion, d'administration et de services à la collectivité reliés à la réalisation de la mission du CSSHC et de ses établissements, et ce, dans l'exercice des fonctions de chacun des utilisateurs.

8.1.4 Usage à des fins personnelles

Les utilisateurs peuvent néanmoins faire usage de certaines ressources informatiques à des fins personnelles à certaines conditions, notamment :

- l'utilisation doit se faire en dehors des heures de prestation de travail et ne pas entraver la performance au travail de l'employé ou celle des autres employés;
- l'utilisation ne doit pas nuire aux opérations du CSSHC, ni à l'efficacité ou à la disponibilité du système informatique;
- l'utilisateur doit assumer, le cas échéant, les frais d'utilisation des équipements et du matériel consommé;
- l'utilisation ne doit pas être à des fins commerciales, lucratives, de propagande ou contraire à la loi;
- doit respecter les ententes pour le prêt de matériel;
- doit respecter les dispositions de la présente politique.

8.1.5 Limite à la vie privée des utilisateurs

En tout temps, les informations ou communications transmises ou reçues par internet sont présumées être de nature professionnelle et concerner les affaires du CSSHC. 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.

8.1.6 Pertes, dommages et inconvénients

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, ou par des gestes ayant pour effet de désactiver, dévier ou contourner n'importe quel système de sécurité du CSSHC.

L'utilisateur doit prendre des mesures de nature à éviter la perte, le vol, la destruction et la détérioration des ressources informatiques. Le CSSHC ne peut s'engager à remplacer un équipement perdu, volé, détruit ou endommagé s'il juge que l'usage a été « abusif ».

Les ressources informatiques fournies par le CSSHC et mises à la disposition de l'utilisateur demeurent en tout temps la propriété du CSSHC, et l'utilisateur s'engage à les rendre sur demande.

Le CSSHC n'assume aucune responsabilité, directe ou indirecte, pour les pertes, dommages ou inconvénients causés aux utilisateurs ou à leurs biens à l'occasion ou en conséquence de l'utilisation des ressources informatiques, ou advenant le cas où il 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.

L'utilisateur ayant en sa possession un ou des appareils mobiles appartenant au CSSHC (ordinateur portable, téléphone, tablette, etc.) s'engage à ne pas apporter ces appareils à l'extérieur du pays et assume toute responsabilité s'il contrevient à cette règle.

8.1.7 Accès non autorisé

Il est interdit d'accéder ou de tenter d'accéder à des fichiers, banques de données, systèmes, réseaux internes ou externes par l'utilisation non autorisée du code d'accès ou du mot de passe d'un autre utilisateur.

L'absence de restrictions d'accès à des données n'implique pas nécessairement pour un utilisateur le droit de les consulter. Entre autres, l'utilisateur doit s'abstenir de consulter et de copier les données affichées ou disponibles à partir d'un poste de travail laissé sans surveillance d'un autre utilisateur, que ces données soient accessibles avec ou sans code d'accès ou de mot de passe.

8.1.8 Utilisation de la langue française

Les utilisateurs doivent respecter la [Politique linguistique](#) dans le cadre de l'utilisation des ressources informatiques. Un français exemplaire doit être employé par le CSSHC et ses employés, et valorisé chez les élèves et leurs parents.

8.2 Droit d'auteur et propriété intellectuelle

8.2.1 Utilisation

En tout temps, l'utilisateur doit respecter les termes et conditions de tout type de licence liant le CSSHC, ainsi que les droits 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 du courrier électronique, le contenu textuel ou multimédia, les émissions de radio et de télévision, la musique, des photos ou graphismes, les logiciels, les compilations, les logos et les marques de commerce disponibles par réseau ou tout autre support numérique.

Dans certaines circonstances, les actions suivantes peuvent contrevenir au respect du droit d'auteur et 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 ou une œuvre cinématographique, afficher l'œuvre artistique d'un tiers, et ce, lorsque des œuvres sont protégées par le droit d'auteur.

Les reproductions de logiciels, de banques de données et informations (textuelles, sonores, symboliques ou visuelles) ne sont autorisées qu'à des fins de copies de sauvegarde ou selon les termes de la licence d'utilisation qui les régit. Personne ne doit les utiliser pour d'autres fins sans le consentement du propriétaire des droits d'auteur.

8.2.2 Création

Conformément à la Loi sur le droit d'auteur, le CSSHC est titulaire des droits se rapportant à toute œuvre créée par les employés dans l'exercice de leurs fonctions, dans la mesure prévue par la loi.

8.3 Outils de travail et de communication

8.3.1 Courrier électronique

Le CSSHC alloue une adresse de courrier électronique à tous les membres du personnel ainsi qu'aux élèves. L'utilisateur reconnaît qu'il a la responsabilité de consulter régulièrement sa boîte courriel pour prendre connaissance des informations.

Ce compte courriel appartient au CSSHC et non à l'utilisateur. Il doit être utilisé à des fins professionnelles. Il est de la responsabilité de l'utilisateur d'éviter d'utiliser le compte courriel de l'organisation pour un usage personnel.

Le CSIO se réserve le droit de bloquer un compte courriel appartenant à l'organisation si nos systèmes détectent un usage pouvant compromettre la sécurité ou l'intégrité du CSSHC (par exemple si lien avec des acteurs frauduleux, activité suspecte sur les médias sociaux, etc.).

L'usager doit s'identifier à titre de signataire de son message et préciser, s'il y a lieu, sa fonction et son lieu de travail, pour tout message électronique diffusé sur le réseau du CSSHC, le tout en conformité avec les normes visuelles mises en place par le service des communications.

Il est interdit de diffuser des messages de façon anonyme ou en utilisant le nom d'une autre personne sans son accord. L'utilisateur doit tenir un langage courtois, respectueux et éthique dans ses échanges par courriel. Il faut se rappeler que les courriels peuvent faire l'objet d'une demande d'accès à l'information.

L'utilisateur doit respecter la confidentialité des messages échangés dans le réseau et s'abstenir d'intercepter, lire, modifier ou détruire tout message qui ne lui est pas destiné.

Il est de la responsabilité de l'utilisateur d'effectuer un élagage régulier de sa boîte de réception pour conserver uniquement les courriels nécessaires à son travail.

L'utilisateur doit être conscient que les courriers électroniques qu'il envoie peuvent, à son insu, être redirigés, imprimés, sauvegardés ou affichés sur des médias ou des systèmes informatiques de tiers. L'utilisateur doit détruire le document si celui-ci ne lui est pas destiné, et en informer l'expéditeur immédiatement.

Le CSSHC encourage les utilisateurs à utiliser l'option réponses automatiques pour signaler les absences et congés du travail.

En cas d'absence et lorsque les circonstances le justifient, les courriels de l'utilisateur seront accessibles à son supérieur immédiat. Celui-ci devra aviser le propriétaire du compte et programmer une réponse automatique en indiquant le nom du remplaçant.

La direction ainsi que le personnel des établissements doivent demeurer vigilants quant à l'usage que font les élèves du courrier électronique. Tout propos haineux ou malveillant ne doit pas être toléré.

8.3.2 Téléphone de bureau et boîte vocale

Le téléphone de bureau et la boîte vocale appartiennent au CSSHC et non à l'utilisateur. Ils doivent être utilisés à des fins professionnelles.

En cas de remplacement pour une absence, la boîte vocale d'un utilisateur deviendra accessible à son remplaçant à la suite de l'autorisation du supérieur. Ce dernier devra faire une demande de modification auprès du STI afin de réinitialiser le mot de passe.

Lors de période de vacances, l'utilisateur a la responsabilité d'activer un message informant de son absence ainsi que la date de son retour, dans la mesure où celle-ci est connue. Au moment du retour, il doit remettre son message d'accueil régulier.

L'utilisateur doit respecter la confidentialité des messages téléphoniques et s'abstenir d'intercepter, modifier ou détruire tout message qui ne lui est pas destiné.

Plusieurs documents complémentaires sur le sujet sont disponibles dans SharePoint (intranet) du CSSHC, tels que des guides d'utilisation, listes des postes téléphoniques, option téléphonie TEAMS, etc.

8.3.3 Téléphone cellulaire

a) Prêt d'appareil

Le CSSHC fournit un téléphone cellulaire aux membres du personnel dont la fonction justifie que ceux-ci soient joints en tout temps et de façon urgente.

Pour l'octroi d'un téléphone cellulaire, une demande devra être adressée à la direction du STI et à la direction générale par la direction de l'établissement ou service concernée.

Au moment où l'appareil et ses accessoires sont remis à l'utilisateur, il s'engage à prendre connaissance de la présente politique.

Un utilisateur qui a un solde qui dépasse le tarif du contrat en vigueur par l'achat d'un service/application ou d'un usage qui va au-delà des limites de données offertes devra rembourser le montant excédentaire sur sa paie, à moins d'avoir démontré que l'utilisation est directement liée à son emploi. Si les frais supplémentaires sont associés à son travail, l'utilisateur a sept jours pour justifier le tout en répondant à l'avis provenant du secrétariat du STI.

Au moment du départ de l'utilisateur, celui-ci doit remettre le téléphone cellulaire et accessoires qui lui avait été initialement remis. Après entente avec la direction du STI, l'utilisateur peut conserver son numéro de téléphone du travail.

b) Appareil ou forfait personnel

Un utilisateur admissible peut également utiliser son cellulaire personnel dans le cadre de son travail. Toutefois il devra utiliser le forfait fourni par le CSSHC. Dans des circonstances exceptionnelles, et ce pour une durée limitée, une entente pourra être prise avec le STI pour éviter le paiement d'une pénalité prévue à un forfait personnel. Dans ce cas, le CSSHC remboursera à l'utilisateur le même montant qu'il paie pour un forfait « CSSHC ».

Par ailleurs, il devra accepter que le CSSHC sécurise les applications professionnelles sur son appareil et fournir son numéro de téléphone afin que celui-ci soit inscrit dans la liste téléphonique du CSSHC.

Seuls les appareils respectant les normes de sécurité et pouvant obtenir les mises à jour du fabricant peuvent être utilisés.

L'utilisateur devra s'engager à maintenir à jour son appareil et ses applications.

c) Sécurité sur les téléphones cellulaires

Les téléphones cellulaires de l'organisation sont gérés par une console de gestion qui permet de mettre à jour des appareils et des applications supportées par le CSSHC (exemple : Outlook, TEAMS, etc.).

La console de gestion empêche l'installation et l'utilisation de certaines applications qui sont interdites par le ministère de la Cybersécurité et du Numérique.

Tout autre téléphone cellulaire utilisé pour accéder aux services ou données du CSSHC doit se conformer aux règles de sécurité en vigueur.

8.3.4 Ordinateur portable et tablette

a) Membres du personnel

Sur recommandation du supérieur, un ordinateur portable ou une tablette est fourni à un membre du personnel qui, dans le cadre de ses fonctions, doit utiliser l'informatique pour réaliser ses tâches. Selon le travail à effectuer, la direction déterminera, avec l'aide du STI, le type d'appareil qui sera fourni à l'utilisateur ainsi que le cycle de renouvellement. Les modalités liées à l'octroi et à la remise prévues au Guide de gestion des équipements informatiques s'appliquent.

Au moment où les équipements seront remis à l'utilisateur, celui-ci devra s'engager à prendre connaissance de la présente politique.

b) Élèves

Dans le cadre de la mesure d'accessibilité aux technologies de l'information et de la communication (mesure 30810), la direction des Services éducatifs peut fournir des outils technologiques à un élève nécessitant un soutien particulier. Le type d'équipement sera déterminé en fonction des besoins de l'élève et avec la collaboration des professionnels impliqués dans le dossier.

Au moment où les équipements seront remis, l'élève et ses parents devront, après avoir pris connaissance de la présente politique, remplir et signer le formulaire de prêt de matériel informatique. Si ceux-ci refusent de signer le formulaire, l'élève aura accès aux équipements seulement sous la supervision d'un enseignant à l'école.

Une vérification des appareils sera effectuée annuellement et au besoin par un membre de l'équipe du STI.

8.3.5 Mozaïk-Portail

Dans le souci de toujours améliorer la communication entre le milieu scolaire et les parents, le CSSHC encourage fortement l'utilisation du portail Mozaïk par les directions d'établissement et par les enseignements, lesquels peuvent y publier notamment les devoirs et les leçons ainsi que les différents résultats en cours d'étape.

Le bulletin scolaire sera disponible en ligne sur le portail Mozaïk à la fin de chacune des étapes. Un parent qui ne dispose pas d'une adresse courriel peut faire une demande à l'école de son enfant pour obtenir une copie papier du bulletin. Par le portail Mozaïk, le parent pourra également consulter ses états de compte et obtenir des informations générales sur les activités de l'école et motiver les absences de son enfant, etc.

Il est de la responsabilité du parent de consulter régulièrement ce portail afin d'être informé de la vie scolaire de son enfant. Il doit à cet effet conserver son code d'accès et son mot de passe confidentiel. En aucun cas, le parent ne doit donner ces informations à son enfant.

Les élèves sont également invités à utiliser Mozaïk-Portail pour accéder à des ressources pédagogiques, prendre connaissance de leur horaire et de leurs résultats scolaires.

8.3.6 Sites Web

a) Site Web du CSSHC

Le CSSHC dispose d'un site Web afin de communiquer divers renseignements à la population : <https://csshc.gouv.qc.ca/>.

La responsabilité de ce site relève du service des communications.

b) Établissements

Chaque établissement dispose d'un site Web. La direction de l'établissement a la responsabilité de mettre à jour les informations de son milieu.

8.4 Confidentialité et protection des renseignements

8.4.1 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 CSSHC 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 du Québec*.

Tout utilisateur est invité à consulter la *Directive relative aux règles encadrant la gouvernance du CSSHC à l'égard des renseignements personnels* pour obtenir plus d'informations sur les exigences légales et principes applicables en matière de protection des renseignements personnels tout au long de leur cycle de vie.

Notamment, advenant qu'un utilisateur ait connaissance d'un incident de confidentialité en lien avec des renseignements personnels, il doit en informer le responsable de la protection des renseignements personnels du CSSHC par courriel à l'adresse suivante : incident.confidentialite@csshc.gouv.qc.ca.

Par ailleurs, toute personne œuvrant au CSSHC doit exceptionnellement déroger du principe de confidentialité des renseignements personnels lorsqu'une communication est nécessaire pour en vue de prévenir un acte de violence, dont un suicide, par un membre du personnel. Les modalités sont plus amplement détaillées dans la [*Directive relative à la communication de renseignements personnels en vue de prévenir un acte de violence, dont le suicide*](#).

9. UTILISATION DES MÉDIAS SOCIAUX

Le CSSHC, par sa mission éducative, reconnaît la valeur et les opportunités créées par les médias sociaux. Il est favorable à l'utilisation des médias sociaux par les membres de son personnel ainsi que par toute personne intéressée à participer à la vie numérique, à partager leur expertise et à faire rayonner la mission et les valeurs de l'organisation, dans la mesure où les comportements s'exercent dans le respect de la nétiquette, des lois et des individus. Plus spécifiquement, les membres du personnel ainsi que toute personne appelée à œuvrer auprès d'élèves mineurs ou handicapés ou à être en contact avec eux se doivent de respecter le [Code d'éthique](#).

9.1 Principes généraux

9.1.1 Faire preuve de jugement, de discernement et de civilité

Tout utilisateur de médias sociaux est personnellement responsable du contenu qu'il publie ou partage. Un jugement critique se doit d'être exercé et tous doivent faire preuve de discernement et de vigilance en tout temps. La ligne entre le rôle professionnel et personnel peut être floue pour une tierce personne. La prudence est de mise. À l'inverse, il importe de prendre du recul avant de juger les écrits des autres. Plusieurs éléments doivent être mis en perspective avant de se forger une opinion et de juger de l'intention de l'autre. L'impolitesse, le dénigrement, le sarcasme, la médisance et le manque de respect n'ont pas leur place. Cela est vrai en personne, mais également lorsque l'on échange sur les médias sociaux.

9.1.2 Le droit de ne pas voir son identité usurpée

Les employés, les élèves et toute autre personne ont droit au respect de leur vie privée et ont droit à la protection de leur dignité, de leur honneur et de leur réputation. La direction de l'école peut agir de façon à faire cesser une atteinte à l'un de ces droits, que cette atteinte soit faite via un site Web, une autre forme de publication ou lors de discussions de corridor.

Il découle de ces principes qu'il est interdit d'usurper l'identité de quelqu'un pour créer une fausse page sur un réseau social à son sujet ou d'utiliser son identité pour poser des gestes sur le Web (par exemple, participer à un blogue ou s'inscrire sur un site de rencontre en ligne). Face à une telle situation, si l'atteinte est réalisée en lien avec les fonctions occupées par l'employé ou en lien avec les relations entre les élèves à l'école, la direction de l'école et/ou le CSSHC doivent agir pour faire cesser l'atteinte.

9.1.3 Le droit de ne pas voir diffuser des images de soi (photo ou vidéo) sans son consentement

Les employés, les élèves et toute autre personne ont le droit de décider si une image d'eux-mêmes peut être ou non diffusée sur le Web, dans la mesure où la photo ou vidéo en question permet d'identifier cette personne. On ne peut pas prendre ni publier une telle photo ou vidéo sans ce consentement. Dans le cas d'un élève mineur, ce consentement est donné par le parent.

9.2 Principes applicables aux membres du personnel

9.2.1 Le rôle de modèle face aux élèves, pendant et en dehors des heures de travail

Tous les membres du personnel, et surtout les enseignants, exercent un rôle de modèle auprès des élèves. Ce rôle s'exerce à l'école, mais également à l'extérieur de celle-ci. Ainsi, le comportement inapproprié d'un employé à l'extérieur de l'école affecte son rôle de modèle s'il est porté à la connaissance des élèves, des parents ou de la population et cela peut justifier l'employeur d'intervenir. Il se doit d'agir avec réserve et absence de familiarité avec les élèves.

Les parents et le public en général s'attendent à ce que les enseignants et autres membres du personnel à qui leurs enfants sont confiés adoptent un comportement cohérent avec leurs fonctions.

9.2.2 L'obligation générale de civilité envers les collègues, les élèves et les parents

Les membres du personnel du CSSHC doivent maintenir une distance professionnelle avec les élèves, et ce même à l'extérieur des heures de classe. En ce sens, toute communication avec un élève par le biais des réseaux sociaux à l'extérieur du cadre scolaire est à éviter.

Les membres du personnel du CSSHC qui utilisent les médias sociaux se doivent d'exercer une grande prudence en veillant à disposer des paramètres de sécurité et de confidentialité très élevés afin d'éviter d'être facilement retracés par les élèves. Il convient aussi d'être prudent quant aux informations (textes, photos, vidéos...) affichées sur les médias sociaux. Les intervenants scolaires exercent un rôle de modèle auprès des élèves. Ce rôle s'exerce à l'école, mais il s'exerce également à l'extérieur de celle-ci, notamment sur les médias sociaux. La direction de l'école a le droit et le devoir d'intervenir auprès des employés, des élèves, des parents ou de toute autre personne présente dans le milieu, pour assurer la civilité.

De plus, les membres du personnel du CSSHC doivent faire preuve de réserve et de modération dans la manifestation publique de leurs opinions en s'abstenant de tenir des propos qui concernent le CSSHC ou ses établissements, ses partenaires, ses employés, ses élèves ou leurs parents et pouvant causer préjudice à leur image ou à leur réputation, et en s'abstenant de tenir des propos pouvant susciter la controverse, qu'ils soient ou non en lien avec le CSSHC.

Seules les personnes autorisées à parler au nom du CSSHC à titre officiel peuvent le faire sur les médias sociaux.

Par ailleurs, nul ne doit faire usage de l'information à caractère confidentiel qu'il obtient dans l'exécution ou à l'occasion de son travail au CSSHC, notamment de l'information qui concerne la situation d'un élève.

L'utilisation des médias sociaux ne peut être encouragée auprès des élèves n'ayant pas l'âge minimum reconnu pour accéder à ces sites.

Toute utilisation personnelle des médias sociaux doit avoir lieu à l'extérieur des heures de travail.

9.2.3 L'obligation de l'employeur de protéger ses employés contre le harcèlement psychologique

Le CSSHC doit prendre les moyens raisonnables pour prévenir le harcèlement psychologique qui peut notamment avoir lieu via les médias sociaux et, lorsqu'une telle conduite est portée à sa connaissance, pour la faire cesser. Le harcèlement psychologique peut être fait par un élève, par un collègue de travail, par un parent ou par une autre personne avec qui l'employé interagit dans son contexte de travail. Aucune forme de violence, d'intimidation ou de harcèlement via les réseaux sociaux ne saurait être tolérée et doit être vivement dénoncée, le tout conformément à la [Politique en matière de violence et de harcèlement psychologique ou sexuel au travail](#).

10. UTILISATION DE L'INTELLIGENCE ARTIFICIELLE

L'utilisation de l'intelligence artificielle générative (IAG) doit toujours être au service de la mission éducative du CSSHC et vise le développement des compétences et l'acquisition des connaissances chez les élèves.

D'emblée, tout utilisateur doit respecter l'âge minimum requis pour l'utilisation d'un système d'IAG. Il doit également prendre connaissance au préalable des modalités d'utilisation et de sécurité applicables et s'assurer qu'elles sont conformes et acceptables. Chaque utilisateur est responsable de faire valider l'outil d'IAG par le CSSHC avant d'y avoir recours.

Il est proscrit de fournir tout renseignement personnel ou information sensible ou confidentielle à un système d'IAG, à moins qu'une utilisation spécifique soit approuvée par le responsable de la protection des renseignements personnels du CSSHC.

L'utilisateur d'IAG doit respecter les droits d'auteur relativement aux informations que l'on soumet à l'IAG. Si l'utilisateur transmet à l'IAG une œuvre protégée par les droits d'auteur, il doit s'assurer de détenir ces droits qui lui permettent de reproduire l'œuvre.

Enfin, chaque résultat issu de l'utilisation de l'IAG se doit d'être validé avec diligence et jugement critique. Par ailleurs, le recours à l'IAG doit être empreint de transparence. Il faut indiquer le nom du système d'IAG et la façon dont il a été utilisé (ex. : « Image générée par le système d'IAG X »).

Pour plus d'informations et pour consulter les normes spécifiques en vigueur, les membres du personnel du CSSHC peuvent se référer à la pastille [Utilisation de l'intelligence artificielle](#) dans la section des ressources informatiques du portail.

11. SANCTIONS

Lorsqu'un utilisateur contrevient à la présente politique, il s'expose à des mesures disciplinaires, administratives ou légales, proportionnelles à la gravité du geste et des impacts de celui-ci sur l'organisation, qui pourrait notamment affecter la confiance du public, le tout conformément aux dispositions applicables des conventions collectives, politiques, règlements, ententes ou contrats, et pour les élèves, au code de vie de l'établissement scolaire qu'ils fréquentent.

De plus, l'une ou plusieurs des sanctions administratives suivantes pourraient être appliquées :

- l'annulation du code d'accès et des mots de passe de l'utilisateur;
- l'interdiction d'utiliser en totalité ou en partie les ressources informatiques, y compris l'accès aux laboratoires de micro-informatique;
- la destruction sans préavis des fichiers constitués contrairement à la présente politique, illégalement ou comportant des informations à caractère illicite;
- l'obligation de rembourser au CSSHC toute somme qu'il serait appelé à défrayer à titre de dommages, de pénalités ou autres à la suite d'une contravention;
- exiger d'un employé qu'il retire toute photo ou commentaire publié sur les médias sociaux en contradiction de la politique.

La direction est responsable de l'application des sanctions, s'il y a lieu, en accord avec la direction des ressources humaines et/ou de la direction générale.

Advenant une vérification de l'utilisation, les droits d'accès d'un utilisateur pourraient être suspendus pour la durée de la vérification. Une telle décision incombe au supérieur immédiat de la personne lorsqu'il s'agit d'un employé ou au directeur d'établissement lorsqu'il s'agit d'un élève.

Par ailleurs, l'utilisateur qui commet un acte illégal s'expose également à une poursuite judiciaire et à une réclamation en dommages.

12. ENTRÉE EN VIGUEUR

Cette politique a été adoptée par le conseil d'administration du Centre de services scolaire des Hauts-Cantons au cours d'une séance tenue le 2 décembre 2025 et entre en vigueur à compter de la date de son adoption.