COMMISSION SCOLAIRE
Eastern Shores
SCHOOL BOARD

POLITIQUE ES-250

ACCÈS AUX TECHNOLOGIES DE L'INFORMATION ET DES COMMUNICATIONS ET UTILISATION ACCEPTABLE

L'UTILISATION DU MASCULIN DANS CE DOCUMENT NE VISE QU'À ALLÉGER LE TEXTE

Adoptée le : 22-06-2022 Résolution : C22-06-872

Table des matières

1. ÉNONCÉ DE POLITIQUE

En appui à son engagement visant à promouvoir et à favoriser l'utilisation des technologies de l'information et des communications (TIC) au cours du processus d'apprentissage et d'enseignement, la Commission scolaire Eastern Shores (CSES) s'engage à :

- veiller à ce que des ressources convenables soient offertes de manière responsable sur le plan financier;
- établir des mécanismes, des politiques et des procédures pour protéger les droits des utilisateurs et veiller à ce que les services et ressources en matière de TIC soient utilisés de façon responsable;
- tenir tous les intervenants responsables de l'utilisation convenable des systèmes de TIC de la CSES;
- sensibiliser continuellement toutes les parties visées à l'utilisation convenable et sécuritaire des TIC;
- restreindre l'accès aux sites Internet dont le contenu est inapproprié.

2. JUSTIFICATION FONDÉE SUR LA RECHERCHE

Michael Fullan (2013) fait référence à l'intégration de la pédagogie, de la technologie et des connaissances sur le changement comme une triade qui compose ce qu'il appelle la « stratosphère ». Bien que chacun de ces facteurs soit individuellement important pour la CSES, la synergie éventuelle des trois, dans une salle de classe contemporaine, l'est davantage encore.

La technologie peut nous aider à « nous ouvrir à un engagement à l'apprentissage et à la résolution globale des problèmes sur une base collaborative » (p. 14). Nous devons « miser sur les prouesses techniques [des étudiants] pour inspirer la confiance, la curiosité, la persévérance et la soif de connaissance » (p. 43). « Les changements en matière de technologie et de pédagogie augmentent incontestablement » (p. 5). [Traduction] La présente politique sur l'utilisation acceptable contribuera à harmoniser ces deux facteurs et servira de cadre pour favoriser leur synergie.

La solution de M. Fullan pour la mise en œuvre d'une « stratosphère » comporte trois volets :

1. L'accent sur l'apprentissage;
2. Le recours à la technologie;
3. La participation de tout le système (p. 74).

Encourager l'utilisation de la technologie par les étudiants et les professeurs nécessite cependant un cadre stratégique qui guidera ces changements. La présente politique sur les technologies de l'information et des communications et leur utilisation acceptable se veut un cadre qui résume les facteurs pédagogiques, technologiques et les connaissances sur le changement pour offrir à la clientèle étudiante de la CSES l'occasion de faire bon usage de la technologie (appareils et réseaux) de façon efficace, sécuritaire et convenable.

3. DOMAINE D'APPLICATION

La présente politique de la CSES sur l'accès aux technologies de l'information et des communications et leur utilisation acceptable (la « politique »), s'applique à l'infrastructure informatique et de télécommunications existante, à l'équipement et aux services fournis ou gérés par la CSES, ou à tout système externe auquel il est nécessaire d'avoir accès pour utiliser ces services, y compris tout logiciel installé sur les systèmes utilisés ou gérés par la CSES. Qui plus est, elle s'applique à toutes les technologies de l'information et des communications (TIC) qui pourraient, à l'heure actuelle ou à l'avenir, être fournies au moyen d'autres sources aux fins d'utilisation par le personnel de la CSES, en personne ou à distance (télétravail). La présente politique s'applique également à tous les intervenants du domaine des technologies de l'information et des communications (employés, étudiants, commissaires, parents, grand public, etc.) qui ont accès aux TIC de la CSES ou les utilisent.

4. OBJECTIF

La CSES reconnaît l'importance des TIC dans le processus d'apprentissage et d'enseignement. L'objectif de la présente politique consiste à:

- promouvoir l'utilisation sécuritaire et convenable des TIC pour toutes les activités éducatives et administratives de la CSES;
- définir les responsabilités respectives de tous les intervenants de la CSES en ce qui a trait à l'utilisation efficace, appropriée, légale, éducative, conforme à l'éthique et liée à l'emploi des TIC;
- assurer la protection des renseignements personnels et organisationnels.

5. RESPECT DES DROITS DE PROPRIÉTÉ ET DE CONFIDENTIALITÉ

1. La CSES étend à tous ses employés le privilège de l'utilisation personnelle raisonnable des systèmes de TIC de la CSES.
2. La CSES est en droit de surveiller tous les registres d'accès et d'utilisation de ses systèmes de TIC, y compris (sans s'y limiter) de surveiller l'accès aux sites Internet, aux fichiers téléchargés et aux courriels. Par conséquent, puisque le privilège de l'utilisation raisonnable des systèmes de TIC de la CSES est étendu aux membres de son personnel, la CSES doit agir de manière discrète et confidentielle au cas où une enquête sur toute éventuelle utilisation inappropriée est menée.
3. Les employés et les étudiants ne doivent pas raisonnablement avoir d'attentes quant au respect de la vie privée lorsqu'ils utilisent les systèmes de TIC de la CSES.
4. Les employés doivent être conscients que tout travail créé ou archivé sur les systèmes de TIC de la CSES, qu'il se rapporte ou non à leurs fonctions professionnelles, demeure la propriété de la CSES, conformément à la *Loi sur le droit d'auteur* (L.R.C., 1985, c. c-42).
5. Les étudiants doivent être conscients que tout travail créé ou archivé sur les systèmes de TIC de la CSES demeure la propriété de l'étudiant, à moins qu'il n'y ait eu entente préalable avec la CSES stipulant le contraire.

6 ÉQUIPEMENT, LOGICIELS ET DEMANDES DE SERVICE

Tout achat et toute installation d'équipement, d'infrastructure ou de logiciels de TIC doit être coordonné ou autrement autorisé par le service de la technologie de l'information conjointement avec, dans certains cas, les services éducatifs, les services d'éducation aux adultes et de formation professionnelle et les administrateurs des établissements scolaires et des centres de formation.

6.1 Équipement

- L'acquisition d'équipement de TIC doit être effectuée par l'entremise du service de la technologie de l'information. Une demande doit être acheminée par courriel à cette fin à l'adresse tech.support@essb.qc.ca, et un préavis d'au moins dix (10) jours ouvrables doit être respecté;
- Tout achat d'équipement de TIC sera déterminé selon la classification d'emploi précisée dans le document sur le matériel informatique qui appartient à la commission scolaire (« Guide organisationnel » – 02.doc);
- L'installation ou la configuration de tout matériel nouveau ou existant de TIC doit être traitée par le service de la technologie de l'information. Une demande doit être acheminée par courriel à cette fin à l'adresse tech.support@essb.qc.ca, et un préavis d'au moins dix (10) jours ouvrables doit être respecté;
- Tout ajout ou toute modification de raccordement au matériel de TIC doit être traité par le service de la technologie de l'information. Une demande doit être acheminée par courriel à cette fin à l'adresse tech.support@essb.qc.ca, et un préavis d'au moins dix (10) jours ouvrables doit être respecté.

6.2 Logiciels

- Tout achat de logiciels, de nature administrative ou éducative, doit être effectué par l'entremise du service de la technologie de l'information. Une demande doit être acheminée par courriel à cette fin à l'adresse tech.support@essb.qc.ca, et un préavis d'au moins dix (10) jours ouvrables doit être respecté;
- Tout nouveau logiciel doit être approuvé par le directeur du service avant l'achat. Une demande doit être transmise par courriel au service de la technologie de l'information à l'adresse tech.support@essb.qc.ca. Les délais varieront selon la complexité du logiciel à évaluer;
- L'installation ou la configuration d'un nouveau logiciel doit se faire par l'entremise du service de la technologie de l'information. Une demande doit être acheminée par courriel à cette fin à l'adresse tech.support@essb.qc.ca, et un préavis d'au moins dix (10) jours ouvrables doit être respecté.

7 RÔLES ET RESPONSABILITÉS DE TOUS LES INTERVENANTS DU SECTEUR DES TIC

Tous les intervenants du secteur des TIC doivent :

1. s'engager à respecter la présente politique, en y apposant officiellement leur signature ou en l'acceptant par voie électronique;
2. s'abstenir de créer, de consulter, d'archiver, de transmettre, de distribuer ou d'imprimer tout document qui est généralement considéré comme étant obscène, de nature pornographique ou érotique, sexuellement explicite, raciste, injurieux, discriminatoire, fondé sur la haine, qui constitue du harcèlement ou des menaces, qui est dégradant ou humiliant, ou autrement discutable en termes d'imagerie ou de niveau de langue;
3. prendre des précautions raisonnables pour empêcher tout accès non autorisé aux systèmes de TIC de la CSES. Ces précautions comprennent le fait de garder confidentiels les identifiants de connexion et les mots de passe, et de verrouiller ou d'empêcher tout accès non autorisé à leur ordinateur lorsqu'ils le laissent sans surveillance pendant de longues périodes;
4. éviter d'archiver des dossiers personnels sur le matériel de la CSES;
5. veiller à ce que One Drive soit relié à Office 365 pour la sauvegarde de fichiers;
6. signaler à tech.support@essb.qc.ca tout matériel reçu ou archivé de toute façon (texte, images, son, etc.) qui semble contrevenir à la politique;
7. respecter et protéger toute information personnelle et confidentielle au sujet d'eux-mêmes et d'autrui;
8. s'abstenir de toute tentative visant à corrompre ou à détruire des données appartenant à la CSES;
9. s'abstenir, par tout moyen que ce soit, d'avoir accès à tout système, service, privilège ou document électronique qu'ils ne sont pas autorisés à consulter;
10. s'abstenir de contrevenir aux lois canadiennes sur le droit d'auteur;
11. s'abstenir d'installer des logiciels non autorisés sur les ordinateurs gérés par la CSES;
12. s'abstenir de recourir aux services de pair à pair ou à toute évolution de ces derniers;
13. respecter toutes les lois et politiques qui précisent l'utilisation appropriée des ordinateurs et du matériel de télécommunications;
14. s'abstenir d'utiliser les systèmes de TIC de la CSES pour en tirer un gain financier personnel. Cela comprend, sans s'y limiter, la sollicitation de fonds et la publicité de biens ou services de tous genres, à moins que cette activité ne soit sanctionnée par la commission scolaire, telle que représentée par le directeur du service dont relève l'employé;
15. demander la permission des administrateurs de l'établissement scolaire ou du centre visé, selon le cas, avant de diffuser toute information qui peut sembler être sanctionnée par la CSES ou qui est liée à des sites Web officiels de la CSES;

16. s'abstenir de transmettre des données de masse non sollicitées (courrier indésirable), y compris des pourriels, de la publicité, des blagues, de la sollicitation, des chaînes de lettres, des alertes de virus, etc.;
17. être conscients qu'il y a une quantité déterminée de bande passante. Les utilisateurs doivent respecter la quantité utilisée par les écoles et les centres. Exemples précis : éviter de télécharger de grandes quantités de contenu vidéo. Éviter également de relier simultanément au réseau tous les postes ou appareils d'une école ou d'un centre.

7.1 Établissements scolaires et centres

Il est de la responsabilité de l'établissement scolaire ou du centre d'éducation aux adultes de veiller à ce qui suit :

1. Les objectifs, avantages et risques éventuels liés à l'utilisation des ressources Internet sont clairement communiqués aux étudiants, aux parents ou aux tuteurs avant qu'un accès ne soit fourni;
2. Les comptes de messagerie ne sont distribués qu'aux étudiants ou à leurs tuteurs respectifs qui ont pris connaissance de l'annexe applicable (II, III ou IV) de la politique et qui l'ont signée;
3. Les activités portant sur l'utilisation des TIC sont planifiées, supervisées et mises en œuvre en fonction de leur valeur éducative;
4. Les ressources en matière de TIC, y compris les sites Internet, sont prévisionnées et leur pertinence est évaluée au vu du programme et des besoins d'apprentissage avant d'être recommandées pour l'usage auprès d'étudiants;
5. On fournit aux étudiants des directives claires pour l'accès Internet, dans le respect des lignes directrices des écoles et des centres;
6. L'utilisation des systèmes de TIC de la CSES est supervisée par les employés de la commission scolaire ou par le personnel autorisé par l'école à superviser les utilisateurs;
7. Surveiller et mettre en vigueur l'utilisation respectueuse des appareils de la CSES (Chromebook, ordinateur portable, tablette, etc.) qui sont confiés aux étudiants.

7.2 Étudiants

Les étudiants doivent s'acquitter des responsabilités suivantes :

1. Soumettre un formulaire signé de consentement ou un formulaire d'entente (annexe II, III ou IV) de la part de l'étudiant, du parent ou du tuteur, indiquant que le signataire s'engage à respecter les modalités de l'accès étudiant;
2. N'utiliser les systèmes de TIC qu'avec la permission ou la supervision du personnel autorisé de la CSES;
3. Ne consulter que du contenu éducatif convenable conforme aux objectifs des affectations de classe et portant sur le cheminement scolaire, tel que déterminé par les professeurs;
4. Signaler immédiatement au personnel enseignant, aux superviseurs ou à l'administrateur toute information, tout message ou tout site Web dont le contenu est inconvenant ou qui les rend mal à l'aise;
5. Obtenir la permission d'un enseignant ou d'un éducateur chargé de la supervision avant d'imprimer du matériel;

6. Manipuler soigneusement les appareils qui leur sont fournis par la CSES, ainsi que leur propre appareil et ceux des autres (Chromebook, ordinateur portable, tablette, ordinateur de bureau et tout autre appareil en leur possession);
7. Les garanties du fabricant s'appliquent aux appareils défectueux, et non aux dommages causés par la négligence ou l'abus des utilisateurs (par exemple, si l'appareil cesse de fonctionner ou ne peut être rechargé). Les étudiants doivent aviser le professeur, qui doit en contrepartie aviser les services techniques en écrivant à l'adresse tech.support@essb.qc.ca;
8. Veuillez noter que les appareils endommagés en raison d'une manipulation incorrecte par les étudiants seront remplacés aux frais des étudiants.

8 PROTECTION DES DONNÉES PERSONNELLES ET CONFIDENTIELLES

À moins d'être autorisés à le faire, il est interdit pour des employés ou tierces parties mandatés par la CSES de transmettre de l'information confidentielle ou nominative par tout moyen électronique. Les employés ou tierces parties mandatés par la CSES ne sont pas autorisés à consulter, à transmettre, à recevoir, à solliciter, à imprimer ou à reproduire des données personnelles ou confidentielles sur l'organisation, ses employés, ses fournisseurs, ses étudiants ou d'autres parties à moins qu'ils n'y soient autorisés par leur description de travail ou par leur employeur, ou en vertu de la *Loi sur l'accès aux documents des organismes publics*.

Les données confidentielles comprennent, sans s'y limiter, les listes des employés ou étudiants, les évaluations du rendement des employés, les détails sur la rémunération, les numéros d'assurance sociale, les mots de passe, les coordonnées et toute autre information qui pourrait causer un préjudice à la CSES, à ses employés ou à ses étudiants si elle était rendue publique.

Les utilisateurs doivent respecter la vie privée d'autrui et s'abstenir d'intercepter des communications et courriels de nature privée qui ne leur sont pas destinés. Le contenu des courriels ne doit pas être modifié, ni altéré ni falsifié. Les utilisateurs ne doivent pas transmettre des données dont l'auteur s'attendrait raisonnablement à ce qu'elles demeurent confidentielles.

9. RESPONSABILITÉ

La CSES n'est pas responsable de toute perte ni de tout dommage causé aux données ou aux appareils des utilisateurs, ni de tout autre problème découlant de l'utilisation de son réseau de TIC.

10. MISE EN VIGUEUR

Les cas d'utilisation éventuelle inappropriée pourraient faire l'objet d'une enquête. La CSES agira avec discrétion et de manière confidentielle. Les enquêtes qui portent sur une utilisation inappropriée peuvent donner lieu à ce qui suit :

1. L'annulation ou un accès restreint aux installations ou aux systèmes de TIC;
2. La divulgation, aux personnes responsables de la CSES ou aux organismes d'application de la loi, des données trouvées pendant l'enquête;

3. Les mesures disciplinaires prises à l'endroit d'employés peuvent inclure un congédiement, selon ce que prévoit la convention collective, les lois applicables et les codes de comportement des établissements scolaires et des centres;
4. Les mesures disciplinaires prises à l'endroit des étudiants peuvent comprendre le fait de révoquer l'adresse courriel de la CSES et l'accès aux appareils et au réseau Internet de la CSES;
5. Tout utilisateur sera tenu responsable des dommages causés au logiciel et/ou au matériel informatique de la CSES en raison d'une négligence grave ou de gestes intentionnels;
6. Advenant le cas où un commissaire fait un usage inapproprié des ressources, le directeur général renverra le dossier au commissaire à l'éthique.

11. GESTION DE L'ACCÈS AU SYSTÈME

Tous les réseaux d'accès Internet de la CSES doivent être munis de noms d'utilisateurs et de mots de passe pour veiller à ce que l'accès soit restreint uniquement aux personnes autorisées. L'autorisation d'accès doit être conforme au processus déterminé dans les énoncés de procédure connexes.

12. MOT DE PASSE POUR TOUS LES UTILISATEURS

Tous les utilisateurs doivent régulièrement changer de mots de passe et adopter des pratiques exemplaires en matière de citoyenneté numérique au sujet de la sécurité et du partage de l'information. Le mot de passe des étudiants peut être réinitialisé par le service de la technologie de l'information.

13. UTILISATION DU SERVICE INTERNET

La CSES fournit aux employés et aux étudiants un accès à Internet pour des activités et des communications qui appuient la mission, la vision et le plan stratégique de la CSES. Tout utilisateur qui enfreint ces règlements et politiques est sujet à des mesures disciplinaires.

13.1 Usage personnel autorisé de l'accès Internet de la CSES – Employés

Les employés peuvent avoir accès aux ressources Internet à des fins personnelles hors des heures de travail. Ils ne sont toutefois pas autorisés à avoir accès aux ressources Internet pour exploiter une entreprise, mener une recherche d'emploi externe, solliciter des fonds pour en tirer un gain personnel, faire campagne pour une cause ou des candidats d'un parti politique, ou promouvoir ou solliciter des fonds à des fins religieuses ou pour d'autres causes personnelles.

13.2 Usage personnel autorisé de l'accès Internet de la CSES – Étudiants

Les étudiants peuvent avoir accès aux ressources Internet à des fins personnelles selon les modalités déterminées par l'école ou le centre. Les étudiants ne sont toutefois pas autorisés à utiliser les ressources Internet pour exploiter une entreprise, mener une recherche d'emploi externe, solliciter des fonds pour en tirer un gain personnel, faire campagne pour une cause ou des candidats d'un parti politique, ou promouvoir ou solliciter des fonds à des fins religieuses ou pour d'autres causes personnelles.

13.3 Confidentialité sur Internet

L'accès à Internet est fourni par la CSES et, en tant que tel, la CSES est légalement en droit de surveiller l'utilisation qui est faite de ce service. Les employés et les étudiants ne doivent donc raisonnablement pas s'attendre à ce qu'on respecte la confidentialité de leurs données lorsqu'ils ont accès à Internet à partir du réseau de la CSES.

14. UTILISATION DU COURRIEL

La CSES fournit aux employés et aux étudiants des outils de communication électroniques, y compris un système de messagerie électronique. La présente politique s'applique à l'accès sur place ou à distance au système de courriel de la CSES et à son utilisation. Les règlements et les politiques de la CSES s'appliquent à tous les utilisateurs qui disposent d'une adresse courriel de la CSES. Tout utilisateur qui enfreint ces règlements et politiques est sujet à des mesures disciplinaires. La CSES permet un accès courriel pour les activités et communications qui appuient la mission, la vision et le plan stratégique de la CSES. Les employés sont autorisés à utiliser le système de courriel de l'organisation à des fins personnelles, mais uniquement dans le respect de la présente politique. Des directives sur les pratiques exemplaires en matière de gestion du courriel se trouvent dans le Guide de l'utilisateur du courriel (annexe VI).

15. CONFIDENTIALITÉ DES COURRIELS

Le système de messagerie électronique est la propriété de la CSES. En tant que tel, la CSES est donc légalement en droit de surveiller l'utilisation qui en est faite. Les employés et les étudiants ne doivent donc raisonnablement pas s'attendre à ce qu'on respecte la confidentialité de leurs données lorsqu'ils utilisent le système de courriel de la CSES.

16. USAGE INAPPROPRIÉ DU SYSTÈME DE COURRIEL

Les employés et les étudiants ne sont pas autorisés à utiliser le système de courriel de la CSES pour prendre part à des activités ou transmettre du contenu (texte, sons et images) qui constituent du harcèlement ou des menaces, sont discriminatoires, obscènes, diffamatoires, douteux ou injurieux selon les lois du Canada et du Québec.

17. UTILISATION DES RÉSEAUX SOCIAUX

Les plateformes et services existants et nouveaux de communication et de collaboration en ligne servent à prendre part à des conversations à l'échelle mondiale. Sur les réseaux sociaux, cependant, la démarcation entre la vie publique et privée, ainsi qu'entre la vie personnelle et professionnelle, peut être floue. Dans la mesure où toute information affichée sur les réseaux sociaux fait partie du domaine public, rien n'empêche donc un employeur de surveiller les activités de ses employés sur Facebook, Twitter et d'autres plateformes semblables. Le devoir de loyauté d'un employé ne se limite pas qu'aux heures de travail et subsiste même après la fin de la relation d'emploi. Par conséquent, un employé n'est pas en droit, même à l'extérieur de ses heures de travail et à partir de son propre matériel informatique, de divulguer de l'information confidentielle au sujet de son employeur ou de divers intervenants, de prendre position ou de faire des déclarations publiques qui peuvent ternir la réputation de l'employeur ou ses activités, ou qui constituent du harcèlement, de l'intimidation ou des menaces envers un agent public ou un collègue de travail. On s'attend à ce que tous ceux qui affichent du contenu sur les réseaux sociaux comprennent les lignes directrices suivantes et s'y conforment.

- **Afficher uniquement des commentaires significatifs et respectueux** (pas de pourriel ni de remarques désobligeantes ou offensantes);

- **Toujours faire une pause et réfléchir avant d'afficher quoi que ce soit**. Ce qu'une personne publie devient largement accessible et pourra être consulté par d'autres. Par conséquent, il faut réfléchir à deux fois avant d'afficher du matériel ou du contenu électronique et déterminer quelles en seront les répercussions à court terme et à long terme;

- **Respecter les renseignements confidentiels, leur contexte et assurer leur confidentialité**;

- En cas de désaccord avec les opinions d'autrui, demeurer poli et bienveillant;

- Utiliser leur vrai nom et préciser quelle fonction ils occupent auprès de la CSES;

- Déterminer clairement s'il existe un intérêt personnel envers le sujet qui fait l'objet d'une discussion.

ANNEXES

ANNEXE I – GLOSSAIRE

Infrastructure : Fondement d'un environnement informatique qui permet de contrôler l'accès à l'information et le flux de l'information au sein de l'organisation par l'entremise de serveurs et de commutateurs réseau.

Intervenant : Toute personne ou tout organisme qui fait directement ou indirectement usage des ressources en matière de technologies de l'information et des communications gérées par la CSES.

Logiciel : Ensemble de programmes et de données connexes renfermant des directives qui permettent le fonctionnement d'un ordinateur.

Matériel ou appareil de TIC : Matériel technologique fourni ou géré par la CSES. Il peut s'agir, sans s'y limiter, de tablettes, d'ordinateurs portables, d'ordinateurs de bureau, de téléphones de bureau, de téléphones cellulaires, de tableaux blancs interactifs ou de projecteurs numériques.

Médias sociaux : Interaction sociale entre des gens qui créent, mettent en commun ou échangent de l'information, des idées, des images et des vidéos au sein de communautés virtuelles et de réseaux.

Pair à pair : Dans le domaine de l'informatique ou du réseautage, fait référence à une architecture d'applications distribuées qui fractionne les tâches ou la charge de travail entre les pairs. Comme c'est le cas pour la plupart des systèmes réseau, des codes non sécuritaires ou sans signature peuvent permettre un accès à distance à des dossiers qui se trouvent sur un poste informatique ou compromettre la sécurité de tout un réseau.

SEAFP : Services d'éducation aux adultes et de formation professionnelle.

Service Internet anonyme : Service Internet qui cache le site auquel on se connecte. Ces services sont utilisés pour contourner les restrictions et les filtres mis en place.

Système de TIC : S'entend de l'équipement et de l'infrastructure des technologies de l'information et des communications de la CSES.

Utilisateur : Toute personne ou tout organisme qui fait un usage direct des systèmes de technologie de l'information et des communications (TIC) de la CSES.

Vidéoconférence : Technologie qui permet à deux ou plusieurs emplacements de communiquer entre eux par le moyen de transmissions audio et vidéo bidirectionnelles (p. ex. Skype, Google Hangouts).

ANNEXE II – Formulaire d'entente – Élèves du primaire

COMMISSION SCOLAIRE EASTERN SHORES
EASTERN SHORES SCHOOL BOARD

FORMULAIRE D'ENTENTE – ÉLÈVES DU PRIMAIRE

- Lorsque j'utilise les ordinateurs de l'école, j'ai de bonnes manières, j'utilise un langage approprié et je ne consulte pas le travail des autres ni ne l'utilise sans leur permission;
- Je ne dois jamais donner de renseignements personnels comme mon adresse, mon numéro de téléphone, l'adresse de mes parents au travail ou leur numéro de téléphone au travail, ou des numéros de carte de crédit;
- Je ne dois pas donner le nom et l'adresse de mon école sans permission;
- Je dois informer immédiatement mon professeur si je trouve de l'information inappropriée ou qui me met mal à l'aise;
- Je ne dois jamais transmettre de photographie de moi ou n'importe quelle autre photographie sans avoir d'abord vérifié avec mes parents ou mon professeur si c'est convenable;
- Je ne dois pas répondre aux messages haineux ou qui me mettent mal à l'aise. Ce n'est pas ma faute si je reçois un message de ce genre. Si cela arrive, je dois en informer immédiatement mon professeur;
- Je ne dois pas donner mon mot de passe à qui que ce soit (même à mon meilleur ami). Mon professeur est la seule personne qui a le droit de connaître mon mot de passe;
- Je ne dois jamais accepter de rencontrer en personne quelqu'un que j'ai rencontré en ligne;
- Je dois parler avec mes parents au sujet des règlements à respecter pour utiliser Internet;
- Je comprends que n'importe qui peut lire les messages que j'envoie et que les travaux que je fais sur l'ordinateur de l'école ne sont pas confidentiels.

J'ai lu et compris ces règlements et je promets de les respecter. Je suis conscient que l'on peut m'enlever mon privilège d'utiliser les ordinateurs de l'école si je ne respecte pas ces règlements.

École de l'élève : _____

Niveau : _____

Nom de l'élève (en lettres moulées) : _____

Signature de l'élève : _____

Date : _____

Date de naissance : _____

La version complète de la présente politique est affichée sur le site Web de la commission scolaire à l'adresse www.essb.qc.ca

Consentement des parents ou des tuteurs

J'ai lu et compris le contenu de la *Politique sur l'accès aux technologies de l'information et des communications et leur utilisation acceptable.* J'accepte que mon enfant ou l'enfant qui se trouve sous ma tutelle ait accès à des services réseau comme le courriel et Internet. Je m'engage à faire tout mon possible pour que mon enfant ou l'enfant qui est placé sous ma tutelle respecte cette politique au meilleur de mes capacités.

Nom du parent ou du tuteur
(en lettres moulées): _____

Signature du parent ou du tuteur : _____

Date: _____

ANNEXE III – Formulaire d'entente – Étudiants de moins de 18 ans

COMMISSION SCOLAIRE EASTERN SHORES
EASTERN SHORES SCHOOL BOARD

FORMULAIRE D'ENTENTE – ÉTUDIANTS DE MOINS DE 18 ANS (DE NIVEAU SECONDAIRE OU inscrits à un CENTRE DE FORMATION PROFESSIONNELLE OU D'ÉDUCATION AUX ADULTES)

Entente conclue avec l'étudiant

J'ai lu et compris les parties qui s'appliquent aux étudiants et que l'on retrouve dans la *Politique sur l'accès aux technologies de l'information et des communications et leur utilisation acceptable*. Je m'engage à les respecter et je comprends que toute violation de ces dispositions peut entraîner la perte de mon privilège d'accès ainsi que la prise de sanctions par mon école ou mon centre.

École ou centre de l'étudiant : _____

Niveau ou programme : _____

Nom de l'étudiant (en lettres moulées) : _____

Signature de l'étudiant : _____

Date : _____

Date de naissance : _____

La version complète de la présente politique est affichée sur le site Web de la commission scolaire à l'adresse www.essb.qc.ca

Consentement des parents ou des tuteurs

J'ai lu et compris le contenu de la *Politique sur l'accès aux technologies de l'information et des communications et leur utilisation acceptable.* J'accepte que mon enfant ou l'enfant qui se trouve sous ma tutelle ait accès à des services réseau comme le courriel et Internet. Je m'engage à faire tout mon possible pour que mon enfant ou l'enfant qui est placé sous ma tutelle respecte cette politique au meilleur de mes capacités.

Nom du parent ou du tuteur
(en lettres moulées) : _____

Signature du parent ou du tuteur : _____

Date : _____

ANNEXE IV – Formulaire d'entente – Étudiants de 18 ans et plus

COMMISSION SCOLAIRE EASTERN SHORES
EASTERN SHORES SCHOOL BOARD

FORMULAIRE D'ENTENTE – ÉTUDIANTS DE 18 ANS ET PLUS

Entente conclue avec l'étudiant

J'ai lu et compris les parties qui s'appliquent aux étudiants et que l'on retrouve dans la *Politique sur l'accès aux technologies de l'information et des communications et leur utilisation acceptable*. Je m'engage à les respecter et je comprends que toute violation de ces dispositions peut entraîner la perte de mon privilège d'accès ainsi que la prise de sanctions par mon école ou mon centre.

École ou centre de l'étudiant : _____

Niveau ou programme : _____

Nom de l'étudiant (en lettres moulées) : _____

Signature de l'étudiant : _____

Date : _____

Date de naissance : _____

La version complète de la présente politique est affichée sur le site Web de la commission scolaire à l'adresse www.essb.qc.ca

ANNEXE V – Formulaire d'entente – Membres du personnel

COMMISSION SCOLAIRE EASTERN SHORES
EASTERN SHORES SCHOOL BOARD

FORMULAIRE D'ENTENTE – MEMBRES DU PERSONNEL

J'ai lu et compris la *Politique sur l'accès aux technologies de l'information et des communications et leur utilisation acceptable.* Je m'engage à la respecter et comprends que toute violation des dispositions qu'elle renferme pourrait entraîner la perte de mon privilège d'accès et la prise de mesures disciplinaires à mon endroit.

École, centre et service de l'employé :

_____

Nom de l'employé (en lettres moulées) :

_____

Signature de l'employé:

_____

Date:

_____

La version complète de la présente politique est affichée sur le site Web de la commission scolaire à l'adresse www.essb.qc.ca

ANNEXE VI – GUIDE DE L'UTILISATEUR DU COURRIEL

INTRODUCTION

Le courrier électronique (courriel) permet de communiquer rapidement et facilement avec un grand nombre de personnes. Les courriels peuvent toutefois être mal utilisés. Voici une liste de choses à faire et à ne pas faire pour rendre l'utilisation des courriels plus sécuritaire et efficace.

SÉCURITÉ DES COURRIELS

Les courriels ne sont pas nécessairement confidentiels. N'incluez pas dans un courriel ce que vous ne souhaitez pas que d'autres voient – soyez également conscient que les lois sur la diffamation s'appliquent aux courriels transmis.

Avant de transmettre des messages qui contiennent des renseignements personnels ou de nature confidentielle, il convient de vous demander s'il est approprié de les envoyer par courriel.

Avant de transmettre un message par courriel, assurez-vous que tous les destinataires ont réellement besoin de recevoir ce message. En outre, soyez prudent lorsque vous transmettez des renseignements confidentiels ou de nature délicate. Il ne faut jamais transmettre des renseignements confidentiels à un auditoire externe ou à des destinataires non autorisés. Avant de cliquer sur le bouton Envoyer, révisez le contenu du message afin qu'il soit convenable pour chaque destinataire.

Virus : Les virus sont souvent transmis par courriel. Vous pouvez réduire la propagation des courriels infectés en ouvrant seulement les courriels qui proviennent de sources fiables et en consultant uniquement les pièces jointes que vous vous attendez à recevoir. Si vous recevez un message suspect, NE L'OUVREZ PAS – il pourrait s'agir d'un virus. Ne consultez que les pièces jointes dont vous êtes certain qu'elles proviennent d'une source à laquelle vous pouvez faire confiance.

Hameçonnage : Il ne faut jamais répondre aux courriels qui demandent de divulguer des renseignements de sécurité personnels. Ce type de pourriel, appelé « hameçonnage », est de plus en plus courant. Il s'agit le plus souvent d'un courriel frauduleux semblant provenir d'un site Web légitime avec lequel le destinataire fait affaire, comme une institution financière. On peut vous demander de vérifier les détails de votre compte en cliquant sur un lien fourni dans le courriel; or, sachez qu'une organisation légitime, comme le service de la technologie de l'information de la CSES, ne vous demandera jamais ce genre de renseignements.

Les services bancaires en ligne et le cybercommerce sont en général sécuritaires, mais il convient d'être prudent pour ce qui est de divulguer des renseignements personnels et organisationnels sur Internet. Les messages d'hameçonnage arborent souvent de vrais logos et semblent provenir d'une organisation qui existe réellement, mais ces messages constituent fréquemment une violation des droits d'auteur et contiennent de fausses adresses. Si vous vous demandez quelle crédibilité accorder à un message, il est plus sécuritaire de décrocher le téléphone et d'appeler l'expéditeur du message pour en confirmer l'authenticité.

Courrier indésirable : Réduisez la quantité de courrier indésirable que vous recevez en étant prudent quand vous divulguez votre adresse de messagerie électronique. Ne transmettez jamais de chaînes de courriels qui révèlent l'adresse courriel de vos collègues à de tierces parties. Soyez prudent en acceptant des offres par courriel ou des envois courriel de fournisseurs. Inscrivez-vous uniquement à des sites Web et à des bulletins dont vous avez réellement besoin.

Ne révélez pas les adresses courriel de vos collègues à des fournisseurs, à des amis ou à d'autres personnes qui ne font pas partie de votre organisation. Faites en sorte que les destinataires indiqués dans les champs « À » *(To)* et « CC » sont autorisés à recevoir vos messages et que vous ne révélerez pas l'adresse courriel d'autres personnes au cours du processus. Ne publiez pas votre adresse courriel, ni celle de vos collègues, sur des forums Internet, des réseaux sociaux, des espaces de discussion ou d'autres espaces publics.

Bien que la CSES ait mis en place un système de filtrage, les attaques informatiques sont de plus en plus complexes et raffinées, et il est difficile de distinguer un courriel d'hameçonnage d'un courriel légitime. Par conséquent, nos systèmes pourraient ne pas les identifier comme étant des pourriels. Les courriels d'hameçonnage contiennent souvent un lien vers un site Web frauduleux qui ressemble à s'y méprendre à un vrai site Web, mais qui a été monté pour voler des renseignements personnels. Pour en savoir davantage et obtenir des conseils à ce sujet, visitez http://www.antiphishing.org/resources/overview/.

ENVOYER UN COURRIEL

Les messages que vous envoyez doivent être courts et simples, et les règles habituelles pour bien écrire s'appliquent. Visez la clarté et la concision, n'exprimez qu'une idée par paragraphe ou section de texte, et veillez au respect des règles d'orthographe et de grammaire.

Pour ce qui est du formatage de vos courriels (p. ex. couleurs, caractères gras, caractères en italiques), vous pouvez l'utiliser uniquement si vous savez que le système informatique du destinataire peut lire ces détails, comme c'est le cas des applications Outlook, Lotus Notes, Hotmail, etc. Certains systèmes plus anciens de messagerie électronique ne peuvent pas du tout déchiffrer ces messages, et les afficheront en texte brut (sans couleurs, ni caractères spéciaux); par conséquent, toute mise en page particulière sera perdue. En pareil cas, utilisez dès le départ le format de texte brut. Cela est particulièrement vrai si vous avez recours à une mise en forme spéciale pour transmettre votre message ou mettre l'accent sur certains éléments.

Faites preuve de prudence lorsque vous envisagez exprimer des sentiments comme le sens de l'humour, le sarcasme ou l'ironie, particulièrement si le message s'adresse à quelqu'un qui ne vous connaît pas. Les émoticônes (visages souriants ou tristes) sont souvent utilisés pour révéler l'humeur de l'expéditeur.

De longs messages (plus de 250 lignes) peuvent ne pas être faciles à lire; il vaut peut-être mieux joindre à votre message un document distinct. (Voir les directives ci-dessous pour transmettre des pièces jointes).

Traiter de plusieurs sujets dans un même message permet de réduire le volume de courriels à envoyer et à échanger. Toutefois, la personne qui reçoit votre message pourrait ignorer un ou plusieurs des sujets abordés. Il est donc préférable que votre message porte sur un seul sujet. Si vous avez besoin d'insérer plusieurs sujets dans un même courriel, veuillez l'indiquer clairement dans la ligne d'objet du message.

Un message transféré ou redirigé comportera généralement différentes sections provenant de différents expéditeurs. Chaque partie du message doit clairement identifier qui l'a écrit, et cette information doit être conservée à mesure que le message circule.

Les messages transférés peuvent devenir volumineux, particulièrement si différentes personnes les ont retransmis et y ont ajouté leurs commentaires. Faites preuve de prudence si vous modifiez le message.

Avant de transférer un courriel, vous pourriez envisager d'informer l'expéditeur du message initial. Cela est d'autant plus important si le message est de nature confidentielle ou si son contenu gagne en volume.

PIÈCES JOINTES

Joindre des fichiers à un courriel est une façon très commode de distribuer des documents, mais cette façon de faire peut sembler difficile à suivre ou peu pratique pour les destinataires. Il est bien de garder à l'esprit les points suivants pour leur faciliter la tâche, plus particulièrement si vous transmettez votre courriel à de nombreuses personnes (par exemple, si vous utilisez une liste d'envoi).

Évitez de joindre des documents lorsqu'il suffit d'envoyer un message écrit; une simple note se transmet mieux lorsqu'elle figure directement dans un courriel en format texte. Il est en effet plus facile et plus rapide pour les destinataires de lire le texte qui figure dans un courriel plutôt que d'ouvrir une pièce jointe.

Veillez à ce que tous les destinataires soient en mesure de lire les pièces jointes, et à ce qu'ils aient la même version de l'application avec laquelle vous avez créé le document. Si vous ne pouvez pas déterminer avec exactitude si c'est le cas, utilisez un format universel comme Adobe PDF.

N'envoyez pas de pièces jointes volumineuses. La CSES a mis en œuvre un réseau haute vitesse dans toutes ses installations, mais ce ne sont pas tous les destinataires qui ont accès à un réseau semblable. Quelqu'un qui reçoit votre message pourrait ne pas être en mesure de consulter un fichier de trop grande taille.

Lorsque vous transférez un message qui comporte des pièces jointes ou que vous y répondez, évitez de laisser les pièces jointes annexées à votre courriel, à moins que cela ne soit absolument nécessaire. Cela ne fait qu'augmenter la taille du courriel, utilise sans raison des ressources organisationnelles limitées et rend le message difficile à suivre.

ASPECT PROFESSIONNEL DES MESSAGES

Incluez toujours une ligne d'objet dans votre message, afin d'en résumer le contenu sans donner trop ou trop peu de détails. Lorsque l'objet d'un message est trop long, les destinataires ont tendance à faire un tri ou à l'ignorer, sans compter que la ligne d'objet n'est pas toujours affichée au long dans la fenêtre de visualisation du courriel.

Il est facile de transmettre l'impression que vous ne savez pas faire preuve de professionnalisme ou que vous êtes négligent si vous ne suivez pas les principes fondamentaux qui régissent la correspondance commerciale ou d'affaires. Veillez à suivre les règles de grammaire et à bien construire vos phrases lorsque vous composez des messages ou y répondez, et utilisez en tout temps un correcteur orthographique. Évitez de rédiger des sections de texte en MAJUSCULES; cela donne l'impression que vous haussez le ton ou que vous criez. Séparez le texte en paragraphes pour qu'il se présente dans un ordre logique et soit plus facile à lire.

Avant de cliquer sur le bouton **Envoyer *(Send)***, relisez et révisez entièrement le contenu de votre message en portant attention aux fautes de grammaire, aux erreurs de ponctuation et aux erreurs de composition (coquilles). Assurez-vous que le ton de votre message soit convenable.

Les courriels ont tendance à manquer de chaleur humaine, du fait qu'il est difficile de transmettre des émotions par écrit. Pour cette raison, évitez les éléments trop vagues ou qui pourraient être interprétés de

différentes façons par différents destinataires. Il vaut mieux s'en tenir aux principaux faits, aux mesures à prendre ou à l'orientation à suivre. S'il faut donner plus de détails ou d'explications, il est préférable de laisser directement un coup de fil à la personne voulue.

Lorsque vous utilisez la fonction **Répondre** ***(Reply)*** pour simplifier l'envoi d'un nouveau courriel, n'oubliez pas de modifier la ligne d'objet du message en conséquence. Si vous laissez inchangé l'objet du message, cela pourrait être source de confusion pour le destinataire, car il pourrait mal interpréter l'information que renferme votre message.

La plupart des fenêtres Windows n'ont pas la même taille ni les mêmes dimensions qu'une page imprimée. Nous vous recommandons donc d'utiliser de courts paragraphes pour mieux vous faire comprendre. Il sera plus facile pour les destinataires de parcourir votre message, et donc plus facile d'absorber ce que vous dites.

BIEN ADRESSER SON MESSAGE – Destinataires, Copie conforme (CC) et Copie conforme invisible (CCI)

La personne à qui s'adresse principalement le message, et donc celle dont vous attendez une réponse, doit être la première à figurer sur la ligne **À** ***(To)***. Les autres personnes inscrites sur cette ligne sont des destinataires secondaires. Les fonctions Copie conforme (**CC**) et Copie conforme invisible (**CCI**) ***(BCC)*** que l'on retrouve dans la plupart des messageries électroniques vous permettent de transmettre une copie du courriel à d'autres personnes qui doivent être informées, mais qui ne sont pas les destinataires principaux du message et ne sont pas directement visées par l'information qu'il renferme. Lorsque vous transmettez un courriel en copie conforme à quelqu'un, il convient de vous assurer que le message est pertinent pour lui. Si vous avez recours à une liste d'envoi, assurez-vous que toutes les personnes inscrites sur la liste ont besoin de recevoir le courriel et rayez le nom de celles qui n'ont pas besoin d'être incluses. Utilisez avec modération la fonction Copie conforme invisible (CCI) *(BCC)*. Si des sujets de nature délicate nécessitent d'être envoyés en CCI, il peut être préférable de discuter de la question en personne.

Ne prenez pas part à l'échange de messages haineux ou injurieux (guerre d'insultes, flambée) entre des utilisateurs.

Les guerres d'insultes, ou flambées, sont des échanges hostiles de courriels qui sont davantage fondés sur les émotions que le raisonnement, et elles n'ont aucune place en communication professionnelle. Si vous recevez une réponse injurieuse ou vous retrouvez au cœur d'une guerre d'insultes, faites une pause avant de répondre, si vous décidez malgré tout de répondre. Réfléchissez à la situation et répondez de façon rationnelle et non émotive. Cette situation est habituellement mieux réglée en personne.

SAVOIR QUAND UTILISER LE COURRIEL (et quand éviter de le faire)

Le courriel ne doit pas être utilisé pour remplacer une conversation, à défaut de quoi le processus sera inutilement compliqué, prendra du temps et, dans la plupart des cas, ne mènera à rien. Il s'agirait d'une utilisation inappropriée des ressources organisationnelles limitées. Les sujets complexes ne doivent pas être abordés par courriel. Il est préférable d'organiser une courte réunion en personne pour en discuter. Le courriel est une bien piètre substitution à une conversation lorsqu'il faut aborder des sujets délicats, difficiles ou désagréables, comme des enjeux qui se rapportent aux ressources humaines. Les communications sensibles ou épineuses se traitent mieux en personne.

GESTION DE LA MESSAGERIE

Il est recommandé de trier vos messages par ordre de priorité, objet, date, expéditeur et d'autres options pour vous aider à retrouver des courriels importants qui nécessitent votre attention. Selon l'étiquette entourant l'usage du courriel, vous devriez répondre à tous les courriels liés à votre travail dans un délai raisonnable. Généralement parlant, vous devriez donner suite à vos courriels professionnels le même jour, même si c'est uniquement pour mentionner au destinataire que vous avez reçu son message et que vous comptez examiner la question bientôt. À l'occasion, vous pourriez recevoir un fil de discussion renfermant la réponse de plusieurs personnes; prenez toujours connaissance de tout le contenu du fil de discussion avant de répondre.

RÉFÉRENCES

Fullan, Michael. *Stratosphere: Integrating Technology, Pedagogy, and Change Knowledge.* Don Mills, Ont.: Pearson, 2013. [Impression]

APWG: Worldwide coalition unifying the global response to cybercrime.
http://www.antiphishing.org/resources/overview/

Définition (en anglais) de la notion de « guerre d'insultes » (flambée)
http://www.oxforddictionaries.com/definition/english/flame-war

Le présent document s'appuie sur les paramètres définis par la Commission scolaire English-Montréal dans sa politique sur l'utilisation acceptable.
http://www.emsb.qc.ca/en/governance_en/pdf/BoardPolicies/DirectorGeneral/DG-25%20ICT%20Access%20and%20Appropriate%20Use%20Feb%2027%202012.pdf