Commission scolaire English-Montréal English Montreal School Board	
POLITIQUE : TECHNOLOGIE DE L'INFORMATION ET DES COMMUNICATIONS – ACCÈS ET UTILISATION APPROPRIÉE	**CODE : DG-25**
Origine :	Comité d'accès et de sécurité de la technologie (CAST)
Autorité :	Résolution #11-11-23-12.2
Référence(s) :	Antérieurement Code PS-14

ÉNONCÉ DE POLITIQUE

En vue de soutenir son engagement à la promotion et l'utilisation des Technologies de l'information et des communications (TIC) dans le processus d'apprentissage et d'enseignement, la Commission scolaire English-Montréal (CSEM) s'engage à :

- assurer la disponibilité de ressources appropriées de façon fiscalement responsable
- établir des mécanismes, des politiques et des procédures visant à sauvegarder les droits des usagers et d'assurer que les services et les ressources TIC soient utilisés de façon responsable;
- tenir toutes les parties prenantes responsables de l'utilisation appropriée des systèmes TIC de la CSEM;
- sensibiliser continuellement toutes les parties prenantes à l'utilisation appropriée et sécuritaire des TIC;
- restreindre l'accès aux sites Internet au contenu approprié, tel qu'identifié à l'Annexe VII-Filtrage de l'Internet.

CHAMP D'APPLICATION

Cette politique de la *CSEM en matière d'accès et d'usage approprié des TIC,* connue ci-après comme la « Politique », s'applique à l'infrastructure des télécommunications et de l'informatique, aux équipements et services fournis ou gérés par la CSEM, ou tous systèmes externes accédés en utilisant ces services, incluant tout logiciel installé ou fonctionnant avec les systèmes gérés par la CSEM. En outre, elle s'applique à toute TIC qui pourrait actuellement, ou à l'avenir, être offerte par l'entremise d'autres sources pour utilisation à la CSEM directement ou à distance.

La Politique s'applique aussi à toutes les parties prenantes des TIC (employés, élèves, commissaires, parents, public, etc.) qui ont accès ou utilisent les TIC de la CSEM.

Le genre masculin est utilisé tout au long du document sans aucune discrimination, mais pour en faciliter la lecture.

BUT

La CSEM reconnaît l'importance des TIC dans le processus d'apprentissage et d'enseignement.

Le but de cette politique est de :

- promouvoir l'utilisation sécuritaire et appropriée des TIC dans toutes les activités administratives et éducatives de la CSEM;
- définir les responsabilités respectives de tous les intervenants des TIC de la CSEM quant à l'utilisation efficace, appropriée, légale, éthique, éducative et d'embauche ;
- respecter la confidentialité de l'information personnelle et organisationnelle.

CONFIDENTIALITÉ ET DROITS DE PROPRIÉTÉ

1) La CSEM accorde le privilège d'une utilisation personnelle raisonnable des systèmes TIC à tous les employés;
2) La CSEM a le droit de surveiller et de tenir un registre de tous les accès et utilisations de tous ses systèmes TIC, incluant, mais sans limiter, la surveillance des accès aux sites Internet, le téléchargement de dossiers et les systèmes de courriels;

   Par conséquent, étant donné que le privilège d'utilisation raisonnable des systèmes TIC de la CSEM est accordé à ses employés, cette dernière agira discrètement et de façon confidentielle au cas où une investigation d'utilisation non appropriée est requise;
3) Les employés et les élèves ne devraient pas avoir une attente raisonnable de confidentialité lorsqu'ils utilisent les systèmes TIC de la CSEM.;
4) Les employés devraient savoir que tout travail créé ou conservé aux systèmes TIC de la CSEM, qu'il soit ou non relié à leur travail, demeure la propriété de la CSEM le tout, conformément à la Loi sur le droit d'auteur (L.R.C., 1985, c.c-42);
5) Les élèves devraient savoir que tout travail créé ou conservé aux systèmes TIC de la CSEM demeure la propriété de l'élève à moins qu'une entente préalable à l'effet contraire avec la CSEM.

ÉQUIPEMENT, LOGICIELS ET DEMANDES DE SERVICES

Tous les achats et installations d'équipement TIC, Infrastructure ou Logiciel doivent être entrepris, coordonnés ou autorisés par le Service des technologies de l'information en collaboration, en certains cas, avec les Services pédagogiques (SP) le Service d'éducation aux adultes et de la formation professionnelle (SEAFP) ou les directions d'école ou de centres.

Équipement

1) Les achats d'équipement TIC doivent être effectués par le biais des TIC au moyen d'une demande par courriel adressée à ITSupport@emsb.qc.ca, ou par le biais du système Intranet de la CSEM, à l'aide du système « Demande d'ordinateur et d'équipement AV » avec un préavis d'un minimum de dix (10) jours ouvrables;

2) L'installation ou la configuration de nouvel ou équipement TIC existant doit être effectuée par le biais des TIC au moyen d'une demande par courriel adressée à ITSupport@emsb.qc.ca avec un préavis d'un minimum de dix (10) jours ouvrables;

3) Des ajouts de câblage ou des modifications à l'équipement TIC doivent être effectués par le biais des TIC au moyen d'une demande par courriel adressée à TISupport@emsb.qc.ca avec un préavis d'un minimum de dix (10) jours ouvrables.

Logiciels

1) Les achats de logiciels, de nature administrative ou éducative, doivent être effectués par le biais des TIC au moyen d'une demande par courriel adressée à ITSupport@emsb.qc.ca ou par le biais de l'Intranet de la CSEM, à l'aide du système « Demande d'ordinateur ou d'équipement AV » avec un préavis d'un minimum de dix (10) jours ouvrables;

2) Les nouveaux logiciels qui ne figurent pas à, soit http://logicielseducatifs.qc.ca/ ou à l'Édu-Portail des SP, qui sont de nature éducative ou conçus pour être utilisés en classe, doivent être approuvés par, soit les SP ou les SEAFP avant d'être achetés. La demande peut être envoyée par courriel au TIC à ITSupport@emsb.qc.ca. Les échéances varieront dépendant de la complexité du logiciel évalué;

3) L'installation ou la configuration de logiciels doit être effectuée par le biais des TIC au moyen d'une demande par courriel adressée à ITSupport@emsb.qc.ca avec un préavis d'un minimum de dix (10) jours ouvrables.

RÔLES ET RESPONSABILITÉS

Toutes les parties prenantes TIC

Toutes les parties prenantes TIC doivent :

1) adhérer et accepter la Politique, soit par signature formelle ou par acceptation électronique;

2) s'abstenir d'utiliser des services Internet anonymes;

3) s'abstenir de créer, d'accéder, de conserver, d'envoyer, de distribuer ou d'imprimer tout matériel qui est généralement considéré obscène, pornographique, érotique, sexuellement explicite, raciste, abusif, discriminatoire; motivé par la haine, harcelant, menaçant, humiliant ou d'autre matériel inacceptable en images ou langage;

4) prendre des précautions raisonnables pour prévenir l'accès non autorisé aux systèmes TIC de la CSEM. Ces précautions incluent préserver la confidentialité des codes d'accès et des mots de passe ou d'empêcher un accès non autorisé à leurs ordinateurs lorsqu'ils sont laissés sans surveillance pour des périodes prolongées de temps;

5) s'abstenir de conserver des dossiers personnels sur l'équipement de la CSEM;

6) copier des dossiers à l'entreposage central du réseau afin d'assurer que les données aient une copie de sécurité. Les TIC n'offrent des services de récupération de données que pour les dossiers reliés au travail et conservés à l'entreposage du réseau;

7) rapporter à ITSecurity@emsb.qc.ca tout matériel reçu ou entreposé de quelque façon que ce soit (texte, images, son, etc.) qui semble être en infraction avec cette Politique;

8) respecter et protéger l'information personnelle et confidentielle qui les concerne ainsi que d'autres personnes;

9) s'abstenir d'endommager, de tenter d'endommager ou de détruire des données de la CSEM;

10) s'abstenir d'obtenir, par quelques moyens que ce soit, l'accès à tout système, service, privilège ou matériel électronique auxquels ils ne sont pas autorisés;

11) s'abstenir de contrevenir aux lois canadiennes des droits d'auteur;

12) s'abstenir d'installer des logiciels non autorisés sur les ordinateurs gérés par la CSEM;

13) s'abstenir d'utiliser les services Pair à Pair (P2P) ou toute évolution semblable;

14) respecter les lois et les politiques qui spécifient l'utilisation appropriée des ordinateurs et d'autres équipements de télécommunications;

15) s'abstenir d'utiliser les systèmes TIC de la CSEM pour des gains monétaires personnels. Ceci inclut, mais n'est pas limité, à la sollicitation de fonds, la publicité et la vente de biens et de services de tout genre à moins qu'une activité ne soit sanctionnée par la Commission représentée par la direction du service de l'employé;

16) demander l'autorisation des directions d'école ou de centres ou consulter le spécialiste en télécommunications et marketing de la Commission, le cas échéant, avant de donner des informations qui sembleraient être sanctionnées par la CSEM ou reliées aux sites Web officiels du réseau;

17) s'abstenir de transmettre des informations en nombre non sollicitées (Pourriel), incluant le pourriel, la publicité, les anecdotes, la sollicitation, les chaînes de lettres, les alertes au virus, etc.;

18) s'assurer que les dispositifs n'appartenant pas à la CSEM ne soient connectés aux réseaux privés de la CSEM à n'importe quel de ses établissements que seulement après autorisation, en soumettant une demande par courriel à ITSecurity@emsb.qc.ca au moins cinq (5) jours ouvrables avant la date demandée.

Écoles et centres

Il incombe à l'école ou centre de s'assurer que:

1) les buts, les avantages et les risques éventuels associés à l'utilisation des ressources Internet soient clairement expliqués aux élèves, parents ou tuteurs avant d'accorder l'accès à ces ressources;

2) que les comptes courriels ne soient attribués qu'aux élèves ou à leurs tuteurs respectifs qui ont révisé et signé la politique;

3) les activités reliées à l'usage des TIC soient planifiées, supervisées et entreprises sur la base de leur valeur éducative;

4) les ressources TIC, incluant les sites Internet, soient visionnées à l'avance et évaluées pour leur pertinence au programme d'études et aux besoins d'apprentissage avant d'être recommandées pour utilisation par l'élève;

5) les élèves reçoivent des directives précises concernant l'accès à l'Internet, conformément aux directives de l'école et du centre;

6) l'utilisation des TIC de la CSEM soit supervisée par des employés de la CSEM ou des personnes autorisées par l'école à superviser les usagers.

Élèves

Il incombe à l'élève :

1) de soumettre un formulaire de consentement ou d'entente (Annexe III, IV et V) signé par l'élève, le parent ou tuteur, indiquant son accord avec les modalités d'accès par l'élève;

2) d'utiliser les systèmes TIC qu'avec l'autorisation et/ou la supervision du personnel de la CSEM;

3) de rapporter immédiatement aux autorités de l'école toute information, message ou site Web non approprié ou qui le met mal à l'aise;

4) d'obtenir l'autorisation de l'enseignant superviseur ou de l'éducateur avant d'imprimer.

PROTECTION DE L'INFORMATION CONFIDENTIELLE, PROPRIÉTAIRE ET PERSONNELLE

À moins d'être autorisés à le faire, les employés ou les tierces parties travaillant au nom de la CSEM, ne sont pas autorisés à transmettre de l'information confidentielle ou nominative à n'importe quelle partie par le biais de médium électronique. Les employés ou tierces parties travaillant au nom de la CSEM ne sont pas autorisés à accéder, envoyer, recevoir, solliciter, imprimer ou copier des informations confidentielles ou propriétaires concernant l'organisation, les employés, les fournisseurs, les élèves ou d'autres associés à moins d'être désignés en vertu de leur description de tâches ou autorisés à le faire par leur employeur, ou selon la Loi respectant l'accès aux documents détenus par des organismes publics.

L'information confidentielle inclut, mais n'est pas limitée, aux listes d'employés ou d'élèves, aux évaluations du rendement de l'employé, les détails de salaire, les numéros d'assurance sociale, les mots de passe, l'information de contact ou toute autre information qui pourrait porter préjudice à la CSEM, ses employés ou élèves, si elle est rendue publique.

Les usagers doivent respecter la vie privée d'autrui et s'abstenir d'intercepter des communications et des courriels personnels. Le contenu des courriels ne doit pas être altéré aux fins de falsification ou de distortion. Les usagers ne doivent pas transmettre de l'information dont l'expéditeur s'attend raisonnablement à ce qu'elle soit privée.

RESPONSABILITÉ

La CSEM n'assume aucune responsabilité pour tous dommages ou pertes de données de l'usager ou aux dispositifs d'entreposage, ni pour n'importe quels problèmes survenant en utilisant les systèmes TIC.

APPLICATION

Les cas d'utilisation probable non appropriée pourraient être investigués. La CSEM agira discrètement et de façon confidentielle en entreprenant de telles enquêtes.

Les investigations qui révèlent une utilisation non appropriée peuvent mener la CSEM à:

1) annuler ou limiter l'accès aux systèmes TIC;
2) révéler les informations découvertes durant l'enquête aux autorités de la CSEM, ou aux organismes chargés de l'application de la loi;
3) prendre des mesures disciplinaires, incluant un renvoi éventuel, conformément aux procédures d'ententes collectives, de lois applicables et/ou de codes de comportement des écoles ou centres.

L'usager sera responsable des dommages au logiciel de la CSEM et/ou équipement, résultant de négligence grossière ou d'actes délibérés.

Dans les cas d'usage probable non approprié par un commissaire, la question sera soumise, par le directeur général, au comité d'éthique et de déontologie. Ce dernier examinera la question et formulera toutes recommandations jugées appropriées au conseil des commissaires, incluant au commissaire à l'éthique.

GESTION DE L'ACCÈS AU SYSTÈME

Tous les systèmes de la CSEM doivent avoir l'identification et les mots de passe appropriés de l'utilisateur afin d'assurer que l'accès soit restreint aux personnes autorisées. L'autorisation d'accès doit suivre le processus identifié aux énoncés de procédure reliés.

Mots de passe pour tous les usagers, à l'exception des élèves du primaire

Les mots de passe sont utilisés à diverses fins, dont: comptes d'application, comptes Web, comptes courriels, protection d'économiseur d'écran, accès à la boîte vocale et autres. Ils doivent être traités comme information sensible et confidentielle de la CSEM. La CSEM demande, qu'autant que possible, des mots de passe solides soient utilisés (voir exemples ci-dessous). Ceci réduira de façon significative les brèches de sécurité des systèmes TIC de la CSEM et améliorera l'intégrité générale et la confidentialité des données de la CSEM.

Pour les systèmes qui permettent aux usagers de changer leur mot de passe, il est demandé à tous les employés de la CSEM de changer leur mot de passe chaque quatre vingt dix (90) jours. Le système retracera un minimum de cinq (5) anciens mots de passe (vous pourrez utiliser votre premier mot de passe seulement après le sixième changement).

Les mots de passe faibles présentent les caractéristiques suivantes:

- contiennent moins que huit (8) caractères;
- sont des mots d'usage courant, dont : mots trouvés dans un dictionnaire, nom de compagnie, noms de familles, dates de naissance, personnages de fantaisie, suites de mots/chiffres, tels que aaabbb ou 12345, etc.

Les mots de passe solides présentent les caractéristiques suivantes:

- contiennent plus de huit (8) caractères;
- comprennent une combinaison de majuscules et de minuscules, de chiffres et de caractères de ponctuation !@#$%^&*()_+|~-=\`{}[]:";'<>?,./.

  Un exemple de mot de passe solide est: *Ohmy1stubbedmyt0e!@#$%^&*

Il est recommandé que tous les usagers de la CSEM observent ces directives de meilleure pratique:

- ne dévoiler votre mot de passe à PERSONNE. Ne pas dévoiler un mot de passe aux collègues pendant que vous êtes en congé. Les TIC ne demanderont jamais votre mot de passe;
- si une personne demande votre mot de passe, référez-la à ce document ou demandez-lui d'appeler la direction des TIC;
- ne pas utiliser la fonction '*Remember Password*'' des sites Web;
- ne pas écrire des mots de passe et les conserver dans votre bureau.

Mots de passe- Élèves du primaire

Les mots de passe des élèves du primaire ne contiendront pas plus de quatre caractères alphabétiques. Les élèves ne devront pas ou ne seront pas autorisés à changer leur mot de passe durant l'année scolaire.

Chaque mot de passe d'élève sera réinitialisé à nouveau, par les TIC, au début de l'année scolaire avant d'être distribué aux enseignants de l'élève, par le biais du GPI Internet.

CONNECTIVITÉ DU RÉSEAU

Le réseau de la CSEM consiste en deux environnements différents, chacun offrant différents services- spécifiquement, un réseau privé et un réseau public. Ces réseaux sont disponibles par le biais de connection câblée ou sans fil.

Le réseau privé a un plus haut niveau de sécurité; il est géré et suivi régulièrement afin d'assurer la disponibilité, le rendement et la confidentialité des données. L'accès à ce réseau, à n'importe quel établissement de la CSEM, est réservé aux dispositifs gérés par la CSEM ou ceux qui ont été autorisés par la direction des TIC et ce, afin d'assurer la sécurité générale des systèmes et des données de la CSEM.

Au cas où il est nécessaire de brancher des dispositifs n'appartenant pas à la CSEM au réseau privé à n'importe quel établissement de la CSEM, une demande par courriel exposant la justification de la connectivité doit être adressée à ITSecurity@emsb.qc.ca. L'équipement personnel branché au réseau privé de la CSEM sera sujet aux mêmes règles que celles régissant l'équipement de la CSEM.

Le réseau public fonctionne parallèlement au réseau privé et il est conçu principalement pour accorder l'accès à l'Internet et à des employés non affiliés à la CSEM ou la connectivité pour les ordinateurs autres que ceux de la CSEM. Une sécurité minimum est établie et les usagers sont responsables du maintien de la sécurité de leur système par des antivirus, filtres anti-pourriels, etc. En outre, il n'y a pas de garantie de disponibilité ou de rendement

UTILISATION DE L'INTERNET

La CSEM offre aux employés et aux élèves l'accès à l'Internet pour des activités et des communications qui appuient et sont reliées à la mission, à la vision et au plan stratégique de la CSEM. Tout usager qui contrevient à ces règlements et politiques est sujet à des mesures disciplinaires.

L'Annexe VI documente les éléments Internet et la façon dont la CSEM filtre chacun d'entre eux.

Utilisation personnelle autorisée de l'accès à l'Internet de la CSEM – Employés

Les employés peuvent accéder aux ressources Internet pour usage personnel durant les heures non ouvrables. Les employés ne sont pas autorisés à utiliser l'accès à l'Internet de la CSEM pour des opérations commerciales, une recherche externe d'emploi, solliciter des fonds pour gains personnels, faire campagne pour des causes ou candidats politiques, ou promouvoir ou solliciter des fonds pour causes religieuses ou personnelles.

Utilisation personnelle autorisée de l'accès à l'Internet de la CSEM – Élèves

Les élèves peuvent accéder aux ressources Internet pour usage personnel selon les termes déterminés par l'école ou le centre. Les élèves ne sont pas autorisés à utiliser l'accès à l'Internet pour des opérations commerciales, une recherche externe d'emploi, solliciter des fonds pour gains personnels, faire campagne pour des candidats ou des causes politiques, ou promouvoir ou solliciter des fonds à des fins religieuses ou personnelles.

Confidentialité de l'Internet

L'accès à l'Internet est offert par la CSEM et, en tant que tel, la CSEM a le droit légal de surveiller l'utilisation de ce service. Les employés et les élèves devraient avoir une attente raisonnable de confidentialité lorsqu'ils accèdent à l'Internet à partir de la CSEM.

UTILISATION DE COURRIEL

La CSEM offre aux employés et aux élèves des outils de communications électroniques, incluant les services de courriel. Cette politique s'applique à l'accès sur place ou à distance et l'utilisation du système de courriel de la CSEM. Les règlements et politiques du courriel de la CSEM s'appliquent à tous les usagers qui ont une adresse courriel de la CSEM. Tout usager qui contrevient à ces règlements et politiques est sujet à des mesures disciplinaires.

La CSEM permet l'accès au courriel pour des activités et des communications qui appuient et sont reliées à la mission, la vision et le plan stratégique de la CSEM. Les employés ne peuvent utiliser le système de courriel pour usage personnel que conformément à cette politique.

Pour les directives des meilleures pratiques d'utilisation du courriel, consultez le Guide de l'utilisateur de courriel (Annexe IX).

Utilisation personnelle autorisée du courriel

Les employés peuvent utiliser le courriel, soit celui de la CSEM ou leur propre courriel Internet (Yahoo, Hotmail, etc.) pour usage personnel durant les heures non ouvrables seulement.

Confidentialité du courriel

Le système de courriel est la propriété de la CSEM et, en tant que tel, la CSEM a le droit légal de surveiller l'utilisation du système. Les employés et les élèves n'ont aucune attente raisonnable de confidentialité lorsqu'ils utilisent le système de courriel de la CSEM.

Utilisation non appropriée du courriel

Il est interdit aux employés et élèves d'utiliser le courriel de la CSEM pour des opérations commerciales, la recherche externe d'emploi, la sollicitation de fonds pour gains personnels, faire campagne pour des candidats ou des causes politiques, ou la promotion ou la sollicitation de fonds à des fins religieuses ou personnelles.

Les employés et les élèves ne sont pas autorisés à utiliser le courriel de la CSEM pour des activités ou la transmission de contenu (texte, son ou images) harcelant, discriminatoire, menaçant, obscène, diffamatoire ou inacceptable ou offensif selon les lois canadiennes et québécoises.

UTILISATION DE MÉDIAS SOCIAUX

Des plateformes et des services existants ou émergeants de communication et de collaboration en ligne sont utilisés pour prendre part à des conversations mondiales.

Dans les réseaux sociaux en ligne, la distinction entre public et privé, personnel et professionnel, pourrait être vague L'on s'attend à ce que toutes les personnes qui ont recours aux médias sociaux, au nom de la CSEM, comprennent et adhèrent aux directives suivantes.

Elles devraient :

- afficher des commentaires significatifs et respectueux – en d'autres termes, pas de POURRIEL et de remarques offensives. Toujours, prendre le temps de réfléchir avant d'afficher. Ce qu'une personne publie est largement accessible et sera disponible à d'autres. Par conséquent, l'affichage ou la publication électronique de contenu devrait être considéré attentivement pour ses implications et impacts, à court et à long terme.

- respecter l'information confidentielle, le contexte et la confidentialité;

- en cas de désaccord avec les opinions d'autrui, avoir des commentaires appropriés et polis;

- utiliser leurs vrais noms, identifier leur rôle à la CSEM;

- indiquer clairement si elles ont des droits acquis au sujet discuté.

RAPPORT ANNUEL

Le conseil des commissaires recevra annuellement un rapport de l'ACS sur l'application de cette politique.

ANNEXE I – GLOSSAIRE

Partie prenante TIC : toute personne ou organisation qui utilise les ressources technologiques gérées par la CSEM, directement ou indirectement.

Équipement ou Dispositifs TIC : n'importe quelle pièce physique de technologie offerte ou gérée par la CSEM. Celles-ci incluent, mais ne sont pas limitées aux ordinateurs, téléphones de bureau, téléphones cellulaires, tableaux blancs interactifs et projecteurs numériques.

Infrastructure : fondation d'un environnement informatique qui contrôle l'accès et le flot d'information au sein de l'organisation, dont les serveurs et les autocommutateurs du réseau.

Systèmes TIC : tout l'équipement et l'infrastructure de la CSEM.

Usager : toute personne ou organisation qui utilise directement les systèmes TIC de la CSEM.

Logiciel : collection de programmes et de données reliées qui donnent des instructions à l'ordinateur au sujet du travail à accomplir.

Pair à Pair (P2P) : informatique ou réseautage: une structure d'application qui répartit les tâches ou les charges de travail entre pairs. Comme la plupart des systèmes en réseau, des codes non sécurisés et non signés peuvent permettre l'accès à distance à des dossiers de l'ordinateur d'une victime ou même compromettre la totalité du réseau.

Services Internet anonymes : un service Internet qui dissimule le site auquel il est branché. Ces services sont utilisés pour court circuiter toutes restrictions d'accès/filtrage en place.

ANNEXE II – FORMULAIRE D'ENTENTE- ÉLÈVES DU PRIMAIRE

- Lorsque j'utiliserais les ordinateurs de l'école, j'utiliserais de bonnes manières, un langage approprié et je ne regarderais pas ou utiliserais le travail d'une autre personne sans autorisation;
- Je ne donnerais pas d'informations personnelles, telles que mon adresse, mon numéro de téléphone, l'adresse de travail ou le numéro de téléphone de mes parents, carte de crédit;
- Je ne donnerais pas le nom ou l'adresse de mon école sans autorisation;
- J'aviserais immédiatement mon enseignant si je découvre toute information qui est non appropriée ou qui me rend inconfortable;
- Je n'enverrais jamais ma photo ou tout autre renseignement sans consulter d'abord mes parents et/ou mon enseignant ;
- Je ne répondrais pas à n'importe quel message nocif ou qui me rend inconfortable. Je ne suis pas fautif si je reçois un tel message. Si tel est le cas, j'aviserais immédiatement mon enseignant;
- Je ne donnerais mon mot de passe à personne (même à mes meilleurs amis) à l'exception de mon enseignant;
- Je n'accepterais jamais de rencontrer une personne que j'ai "connue" en ligne;
- Je parlerais à mes parents des règlements concernant l'accès en ligne ;
- Je réalise que n'importe qui peut lire les messages que j'envoie et que mon travail sur l'ordinateur n'est pas privé.

J'ai lu et j'ai compris les règlements et promet de les observer. Si je ne les observe pas, je sais que mes privilèges d'ordinateur peuvent être restreints ou supprimés.

École de l'élève _____

Niveau: _____

Nom de l'élève (en majuscules s.v.p.): _____

Signature de l'élève _____

Date: _____

Date de naissance: _____

Une version complète de la politique est disponible au site Web de la Commission à www.emsb.qc.ca

Parent ou Tuteur

J'ai lu et j'ai compris la Politique sur l'accès et l'utilisation appropriée des technologies de l'information et des communications. J'accorde la permission à mon enfant ou pupille d'accéder à des services de réseau, tels que le courriel et l'Internet. Je ferais de mon mieux pour m'assurer que mon enfant adhère à cette politique au meilleur de mes capacités.

Nom du parent ou du tuteur (majuscules s.v.p.): _____

Signature du parent ou du tuteur: _____

Date : _____

ANNEXE III – FORMULAIRE D'ENTENTE- ÉLÈVES DE MOINS DE 18 ANS (ÉCOLE SECONDAIRE OU CENTRE EAFP)

Élève

J'ai lu et j'ai compris la Politique sur l'accès et l'utilisation appropriée de la technologie de l'information et des communications. J'accepte de l'observer et je réalise que toute violation de n'importe quelle disposition pourrait entraîner la perte de mon privilège d'accès et des sanctions de l'école ou du centre.

École ou centre de l'élève: _____

Niveau ou programme: _____

Nom de l'élève (majuscules s.v.p.):_____

Signature de l'élève: _____

Date: _____

Date de naissance: _____

Une version complète de la Politique est disponible au site Web de la Commission à www.emsb.qc.ca

Consentement du parent ou tuteur

J'ai lu et j'ai compris la Politique d'utilisation appropriée des technologies de l'information et des communications. J'autorise mon enfant ou pupille à accéder aux services, tels que le courriel et l'Internet. J'essaierai d'assurer que mon enfant adhère à cette politique au meilleur de mes capacités.

Nom du parent ou tuteur (majuscules svp): _____

Signature du parent ou tuteur: _____

Date: _____

ANNEXE IV – FORMULAIRE D'ENTENTE – ÉLÈVES DE 18 ANS ET PLUS

Accord de l'usager

J'ai lu et j'ai compris la Politique sur l'utilisation appropriée de la technologie de l'information et des communications. J'accepte d'y adhérer et je réalise que toute violation de n'importe quelle disposition pourrait entraîner la perte du privilège d'accès et des sanctions de l'école ou centre.

École ou centre de l'élève _____

Niveau ou programme: _____

Nom de l'élève (majuscules svp):_____

Signature de l'élève: _____

Date: _____

Date de naissance: _____

Une version complète de la politique est disponible au site Web de la Commission à www.emsb.qc.ca

ANNEXE V – FORMULAIRE D'ENTENTE – EMPLOYÉ

Accord de l'employé

J'ai lu et j'ai compris la politique sur l'accès et l'utilisation appropriée de la technologie de l'information et des communications. J'accepte d'y adhérer et je réalise que toute violation de n'importe quelle disposition pourrait entraîner la perte du privilège d'accès et des mesures disciplinaires.

École, Centre, Service de l'employé: _____

Nom de l'employé (majuscules svp):_____

Signature de l'employé: _____

Date :

Une version complète de la politique est disponible au site Web de la Commission à www.emsb.qc.ca

ANNEXE VI – FILTRAGE DE L'INTERNET

Une liste des éléments de l'Internet se trouve ci-dessous et la façon dont la CSEM filtrera chacun d'entre eux.

Accès refusé

Logiciel malveillant
Espion enregistreur de clavier ou enregistreur de frappe
Hameçennage, appâtage et fraude
Logiciel espion
Éviter ou contourner un proxy
Sites de traduction URL
Web et pourriel électronique
Accès à distance
Pair-à pair partage des fichiers
Logiciel indésirable
Annonces/Publicité
Sites Web malintentionnés
Courtage en ligne
Site qui vous paye pour surfer sur le Web
Matériel pour adultes
Illégal ou questionnable
Piratage
Hébergement Web (Internet)
Stockage réseau personnel et sauvegarde
Ventes aux enchères sur l'Internet
Personnel et datation
Chasse sportive et clubs d'armes à feu
Inodore
Armes
Logiciel libre et téléchargement de logiciels

Accès permis

Les éléments suivants ne sont autorisés QUE pour des fins directement reliées au travail d'une personne ou d'une activité éducative.

Affaires et Économie
Éducation
Gouvernement
Courriel organisationnel
Nouvelles et Médias
Évènements spéciaux
YouTube
Tableaux d'affichage et Forums
Technologie de l'information
Moteurs de recherche et Portails
Courriel général
Textos et Médias
Organisations professionnelles et de travail
Organismes de services et philanthropiques
Affiliations et organisations sociales
Société et modes de vie
Outil de courrier
Groupes de pression
Santé
Clavardage
Médicaments prescrits
Restaurants
Réseautage social et sites personnels
Sports
Voyages
Véhicules
Téléphonie Internet- Skype
Radio et TV Internet
Transmission multimédia
Messagerie instantanée
Tableaux d'affichage et forums
Médicaments prescrits
Divertissement
Recherche d'emploi
Passe-temps
Magasinage
Immobilier

ANNEXE VII – DEMANDE DE CHANGEMENT À UN COMPTE D'EMPLOYÉ

Comptes d'usagers

Les changements au compte d'usager incluent des demandes de: créer un nouvel usager, changements à un compte existant (ajouter ou éliminer l'accès aux systèmes, dont GPI, DOFIN, etc.), désactiver temporairement des comptes, demander un nouveau numéro de téléphone et éliminer des comptes. Les demandes de ce genre doivent être faites par le superviseur direct ou le directeur du service de la personne, à l'aide du "**Formulaire de changement de compte d'employé-ePaper.pdf ».**

Le formulaire rempli doit être envoyé par courriel à ITSupport@emsb.qc.ca pour traitement, en donnant un préavis d'un minimum de cinq (5) jours ouvrables. Ce formulaire se trouve à la section des formulaires de l'Intranet de la CSEM.

Demandes de services

Demandes de services autres que les éléments d'appui journaliers, soit, installer de l'équipement pour un atelier, transférer les connexions d'équipement d'un endroit à un autre, etc. Les demandes de ce genre doivent être soumises par courriel à ITSupport@emsb.qc.ca en donnant un préavis d'un minimum de dix (10) jours ouvrables pour traitement.

Exemple de formulaire

Ce formulaire doit être rempli par le superviseur immédiat ou le directeur du service de l'employé chaque fois qu'un accès à un ordinateur dot être créé, supprimé ou modifié. Le formulaire rempli doit être envoyé, par courriel, à ITsupport@emsb.qc.ca avec un préavis de cinq (5) jours ouvrables pour traitement.

Type de demande : ◯ Nouvelle ◯ Départ ◯ Congé temporaire ◯ Changement

Date requise :
(année-mois-jour)

Prénom :

Nom de famille :

Adresse courriel :
(usagers existants seulement)

Nom du Service :

Désactiver le compte : ◉ **Non** ◯ **Oui** **De :** (année-mois-jour)

À : (année-mois-jour)

Supprimer le compte : ◉ **Non** ◯ **Oui** **Date :** (année-mois-jour)

Besoins particuliers de logiciels : ◯ **GPI** ◯ **GPI Internet** ☐ **SPI** ☐ **DOFIN** ☐ **PAIE** ☐ **REGARD** ☐ **AVANT GARDE** ☐ **JADE** ☐ **PORTAIL**

Autres :

Ordinateur : ◯ **Nouveau** ◯ **transfert de :**

Téléphone de bureau : ◯ **Nouveau** ◯ **transfert de :**

Commentaires :

Soumis par : (Nom du superviseur) **Date :** (année-mois-jour)

ANNEXE VIII – GUIDE DE L'USAGER DE COURRIEL

Introduction

Le courrier électronique (courriel) est devenu un moyen important pour communiquer facilement et rapidement avec un grand nombre de personnes. Cependant, le courriel peut être mal utilisé ou abusif. Voici quelques conseils qui permettront une utilisation plus efficace et sécuritaire des courriels.

Sécurité des courriels

- Les courriels ne sont pas nécessairement privés. N'incluez rien dans votre courriel que vous ne voudriez pas montrer à d'autres personnes- en particulier, n'oubliez pas que les lois sur la diffamation s'appliquent aux courriels.

- Avant d'envoyer des messages qui contiennent de l'information sensible ou personnelle, vous devriez considérer si un courriel est approprié.

- Avant de réacheminer un courriel, assurez-vous que tous les destinataires ont besoin de recevoir ce message. En outre, soyez prudent lorsque vous réacheminez une information sensible ou confidentielle. Ne jamais réacheminer une information propriétaire à des personnes externes ou des destinataires non autorisés. Avant de cliquer le bouton « Envoi », assurez-vous que les contenus du message sont appropriés pour chaque destinataire répertorié.

- **Virus**: sont souvent répandus à travers les courriels. Vous pouvez réduire la diffusion de virus de courriels en n'ouvrant que le courriel de sources fiables et n'ouvrir que les pièces jointes que vous attendez. Si vous recevez un message suspect, NE L'OUVREZ PAS, ce pourrait être un virus. En particulier, n'ouvrez que les pièces jointes dont vous êtes sûr qu'ils proviennent d'une source fiable.

- **Filoutage**: Ne jamais répondre à des courriels qui demandent de l'information personnelle. Un type de pourriel surnommé 'Filoutage' est de plus en plus commun, lorsque vous recevez un courriel qui semble provenir d'un site légitime avec lequel vous traitez, telle qu'une institution financière. Il pourrait vous demander de vérifier des détails de votre compte en accédant à un lien du courriel, mais les organisations légitimes, incluant le groupe TIC de la CSEM, ne vous demanderont jamais ce type d'information.

  Les opérations bancaires en ligne et le commerce électronique sont généralement sécuritaires, mais vous devriez toujours être prudent lorsque vous donnez de l'information personnelle et corporative par Internet. Les messages de filoutage présentent souvent de vrais logos et semblent provenir de l'organisation, mais ces messages ne sont fréquemment que des contrefaçons de droits d'auteur et de fausses adresses. Si vous soupçonnez la crédibilité d'un message, vous feriez mieux d'appeler la personne pour en confirmer l'authenticité.

  Bien que la CSEM a mis en place un système de filtrage, les attaques sont de plus en plus sophistiquées et il est difficile de faire la différence entre un courriel légitime et un message de filoutage et nos systèmes pourraient ne pas les

identifier comme POURRIEL. Ils contiennent souvent un lien à un site Web falsifié qui ressemble au vrai site, mais qui a été créé pour dérober de l'information personnelle. Pour plus d'informations et conseils, visitez :

http://www.antiphishing.org/resources.html#advice.

- **POURRIEL**: Réduisez la quantité de pourriel que vous recevez en faisant preuve de prudence lorsque vous affichez votre adresse courriel. Ne jamais faire suivre des messages à chaîne qui révèlent souvent les adresses courriel de vos collègues à d'autres parties. Faites preuve de prudence en acceptant des offres par courriel ou en acceptant des courriels de vendeurs; ne souscrivez qu'aux sites Web et lettres d'information dont vous avez vraiment besoin.

  Ne révélez pas les adresses courriel de vos collègues à des vendeurs, amis ou autres personnes en dehors de l'organisation. Vérifiez que les destinataires répertoriés aux champs A et C devraient recevoir les messages et que vous ne révèlerez pas les adresses courriels d'autres personnes. N'affichez pas votre adresse courriel ou celle de vos collègues aux forums Internet, services ou sites de réseautage social, salles de clavardage ou autres domaines publics.

Envoyer des courriels

- Que vos messages soient courts et simples- les règles usuelles de bonne écriture s'appliquent; soyez clair et concis, n'exprimez qu'une idée par paragraphe ou section, vérifiez votre orthographe et la grammaire.
- N'utilisez la mise en forme spéciale soit, couleurs, caractères gras, italiques, etc., que si vous savez que le système du destinataire peut lire ces détails, soit les personnes utilisant *Outlook, Lotus Notes, Hotmail*, etc. Certains systèmes plus anciens de courriels ne peuvent pas lire du tout ces messages et d'autres les afficheront comme texte simple et toute mise en forme que vous aurez utilisée sera perdue. Dans ce cas, utilisez le format de texte simple. Ceci s'applique particulièrement si vous utilisez la mise en forme pour transmettre un message spécial.
- Soyez prudent lorsque vous utilisez l'humour, le sarcasme ou l'ironie, particulièrement si le message est adressé à une personne qui ne vous connait pas. Les « binettes » (*smileys*) sont souvent utilisées pour transmettre l'humour, etc.
- Les longs messages (plus de 250 lignes) pourraient être difficiles à lire- une pièce jointe serait plus appropriée. (Voir ci-dessous le guide d'envoi de pièces jointes).
- Couvrir de multiples sujets en un message implique moins d'envois et, par conséquent, moins de volume et de trafic de courriels. Cependant, votre destinataire pourrait passer outre à l'un ou plusieurs de ces sujets. Il est préférable de ne couvrir qu'un sujet par message. Si vous avez besoin de couvrir plus d'un sujet par courriel, assurez-vous que ce fait soit indiqué à la ligne du sujet.

- Un message réacheminé ou redirigé aura généralement des sections de divers auteurs. Chaque section devrait identifier clairement la personne qui l'a rédigée et cette information devrait être conservée lors de la transmission du message.
- La taille des messages réacheminés peut augmenter, particulièrement si diverses personnes l'ont réacheminé et ajouté des commentaires; soyez attentif si vous modifiez le message.
- Avant de réacheminer des messages, vous pourriez considérer aviser l'expéditeur du message. Ceci prend de l'importance alors que la sensibilité des contenus du message augmente.

Pièces jointes de courriel

Joindre des dossiers aux courriels est une façon très pratique de distribuer des documents. Mais ceci pourrait poser des difficultés au destinataire; souvenez- vous des points suivants pour faciliter le processus. Ils sont particulièrement importants si vous les envoyez à plusieurs personnes, comme lorsque vous utilisez des listes de distribution.

- N'utilisez pas de pièces jointes lorsqu'un simple texte suffira; il serait mieux d'envoyer un mémo en tant que texte de courriel. Ce procédé est plus rapide et plus facile à lire pour les destinataires que d'ouvrir une pièce jointe.
- Assurez-vous que les destinataires peuvent lire les dossiers joints; assurez-vous que tous les destinataires ont la même version de l'application avec laquelle vous avez créé le document. Si ceci ne peut pas être déterminé avec précision, utilisez un format universel, tels que, Adobe PDF.
- Maintenez la taille des pièces jointes à un minimum. La CSEM a mis en place un réseau à haute vitesse dans tous ces établissements, mais ce n'est pas le cas pour tout le monde. Un destinataire pourrait ne pas pouvoir lire un grand dossier joint. La taille maximum de message permise pour tous les messages entrant ou sortant est de 20MB.
- Lorsque vous réacheminez ou répondez à des messages avec pièces jointes, à moins que ce ne soit absolument nécessaire, évitez de conserver la pièce jointe dans le courriel. Ceci augmente la taille du courriel, utilise inutilement les ressources organisationnelles limitées et rend le message difficile à suivre.

Messages professionnels

Incluez toujours une ligne descriptive du sujet, résumez le message sans être vague. Les longs sujets ont tendance à être parcourus distraitement ou ignorés et ne sont pas toujours proprement affichés par les courriels.

Il est facile de donner l'impression de ne pas être professionnel ou être négligent si vous n'observez pas quelques principes de base de bonne écriture. Assurez-vous d'observer la grammaire et la structure de phrases lorsque vous composez ou répondez à des messages et utilisez le correcteur d'orthographe. N'écrivez pas en LETTRES MAJUSCULES; ceci donne l'impression de crier. Divisez votre message en paragraphes, aux fins de logique et de facilité de lecture.

Avant de cliquer sur la touche « Envoi », relisez tout le message, vérifiez-le pour détecter des erreurs grammaticales, de ponctuation et de frappe. Assurez-vous que le ton de votre message soit approprié. Les courriels ont tendance à sembler impersonnels; les émotions sont difficiles à transmettre par écrit. Pour cette raison, évitez les éléments qui sont vagues ou qui peuvent être interprétés différemment par différents lecteurs. Il est préférable de donner des faits de base et appelez la personne au cas où une explication plus détaillée serait requise.

Lorsque vous utilisez la fonction **Réponse** afin de simplifier l'envoi d'un nouveau courriel à quelqu'un, assurez-vous d'ajuster la ligne « Sujet » en conséquence. Ne pas modifier la ligne « Sujet ». Cela pourrait prêter à confusion pour le lecteur ainsi que donner une mauvaise interprétation de l'information contenue dans le message.

La plupart des fenêtres courriels n'ont pas la même taille et la portée d'une page imprimée. Utilisez des paragraphes plus courts afin de mieux transmettre votre message. Il sera plus facile pour les lecteurs de faire défiler votre message et de mieux l'absorber.

Façon appropriée d'adresser un message (À, CC, et CCI)

La personne principale à qui le message est adressé, ainsi que la personne dont vous attendez une réponse, devraient figurer en premier à la ligne **À**, les autres sont en réserve. Les caractéristiques copie conforme (CC) et copie conforme invisible (CCI) que l'on retrouve chez la plupart des clients courriels vous permettent d'envoyer des copies d'un courriel à d'autres personnes qui ont besoin d'être informées mais qui ne sont pas les destinataires principaux et sont indirectement affectées par l'information du message.

Lorsque vous adressez des copies à d'autres personnes, assurez-vous que le message courriel les concerne. Si vous utilisez des listes de distribution de courriels, vérifiez que tous les membres de la liste devraient recevoir le courriel; éliminez ceux qui n'ont pas besoin d'être inclus. Utilisez la caractéristique CCI avec ménagement. Si des sujets sensibles doivent être transmis en CCI à d'autres personnes, il serait préférable d'en discuter en personne.

Ne participez pas à des fusillades

Les fusillades sont des échanges animés de courriels, qui sont plus émotifs que raisonnés et ils n'ont pas de place dans les communications professionnelles. Si vous recevez une fusillade ou si vous vous trouvez soudainement impliqué dans une fusillade, prenez un peu de temps avant de répondre, si vous comptez y répondre. Réfléchissez à la situation et répondez rationnellement et non émotivement et il est préférable de le faire en personne.

Savoir quand utiliser un courriel (et quand ne pas le faire)

Le courriel ne devrait pas être utilisé pour remplacer une conversation. Lorsqu'il est utilisé à cette fin, l'activité est compliquée sans besoin, longue et, dans la plupart des cas, n'offre aucune solution et c'est une utilisation non appropriée de ressources organisationnelles limitées. Aucuns sujets compliqués ne devraient être « discutés » de cette façon. Organisez plutôt une courte réunion pour aborder le sujet en personne.

Le courriel est aussi un faible moyen de conversation pour des discussions critiques, difficiles et/ou déplaisantes, tels que des problèmes reliés aux questions de ressources humaines. Les communications sensibles sont mieux abordées en personne.

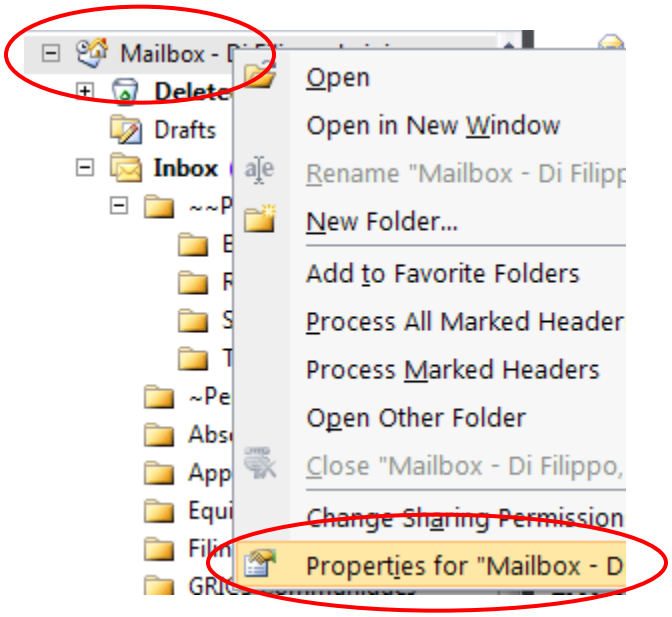
Gérer votre boîte vocale

Il a été alloué 500MB pour l'entreposage des courriels des usagers de la CSEM. Ceci inclut tout l'espace occupé, non seulement pour les messages d'arrivée mais aussi des inscriptions de calendriers, des messages de sortie, des messages classés dans des dossiers créés par les usagers et des messages supprimés.

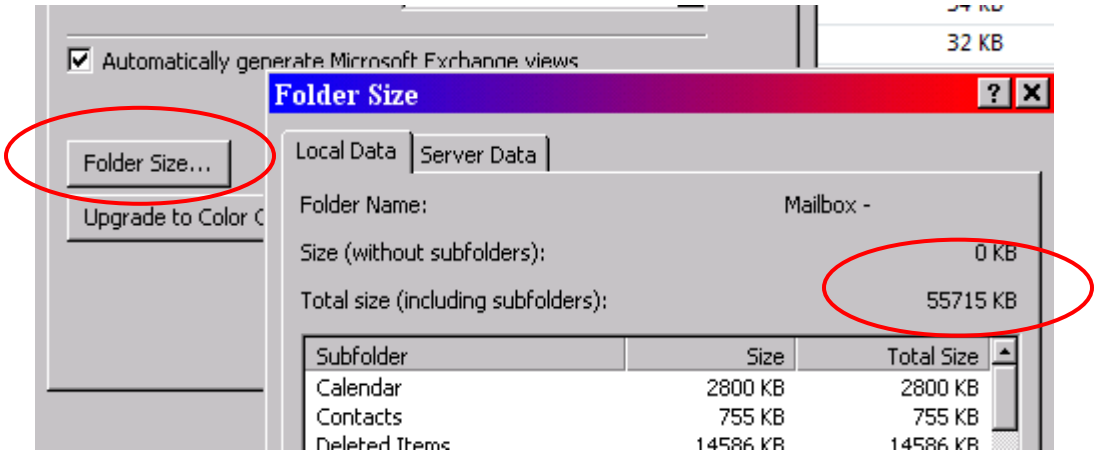
Triez les messages par priorité, sujet, date, expéditeur et autres options qui vous aident à trouver un courriel important qui requière votre attention. L'étiquette appropriée de courriel exige que vous répondiez à tous les courriels à temps. En général, vous devriez répondre à tous les courriels professionnels en un jour ouvrable, même si c'est pour dire que vous avez reçu le message et que vous vous en occuperez. À l'occasion, vous pourriez recevoir une suite de courriels qui contiennent des réponses de diverses personnes; lisez-la toujours en entier avant de répondre.

Vérifiez la taille de votre boîte à lettres

- Ouvrir *Outlook*
- Cliquez droit sur « Boîte à lettres » et choisissez ensuite « Propriétés » de la liste déroulante :

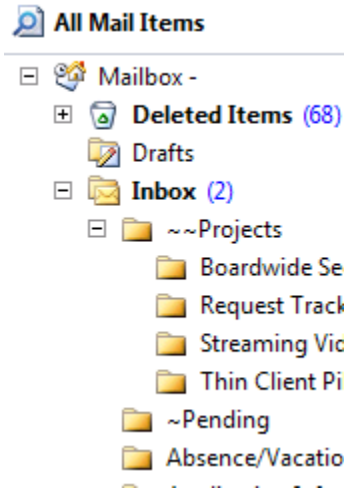


- Dans la fenêtre qui ouvre, cliquez sur la touche « Taille de dossier » au bas de l'écran. Ceci vous indiquera la taille totale de votre boîte à lettres.

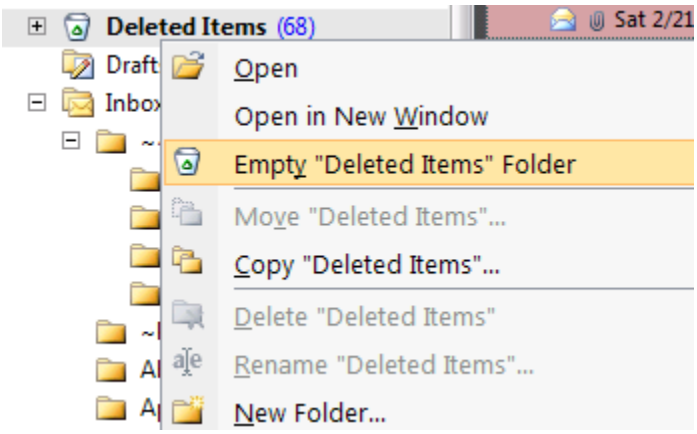


La boîte à lettres est pleine

- Supprimez les courriels ou messages non importants dont vous n'avez plus besoin.
- Réduisez la taille de votre boîte à lettres. Votre boîte à lettres n'est pas seulement votre boite d'entrée mais elle inclut tous les dossiers énumérés : dossiers que vous avez créés, articles supprimés, articles transmis, boîte de sortie, etc.



- Vérifiez les dossiers suivants et supprimez ce qui n'est pas nécessaire. Soulignez les articles à être supprimés, ensuite, appuyez sur « *SHIFT* » et « *Delete* » en même temps pour supprimer ces articles, de façon permanente.
    - **Articles envoyés** (ces articles peuvent être classés dans d'autres dossiers s'ils devraient être conservés); autrement, supprimez le message.
    - **Dossier de sortie**
    - **Articles supprimés** habituellement, vous pouvez supprimer tout le contenu de ce dossier. Pour ce faire, cliquez droit sur le dossier « Articles supprimés » et choisissez « *Empty* » de la liste déroulante.



- Vérifiez votre boîte d'entrée et tout autre dossier de votre boîte à lettres (ceux figurant directement sous votre nom). Supprimez les vieux messages et tout ce que vous n'avez pas besoin de conserver.

Demande d'espace additionnel

Les messages courriels du personnel de la CSEM sont conservés aux serveurs centraux gérés par les TIC. L'espace d'entreposage n'est pas infini et, afin de diminuer les coûts et de simplifier l'administration, un quota de 500MB a été appliqué au personnel. Ceci devrait être suffisant pour la majorité des personnes, à condition qu'elles gèrent leur boîte aux lettres de la façon exposée ci-dessus.

Dans des circonstances exceptionnelles, si le quota n'est pas suffisant et ne permet pas à une personne de s'acquitter proprement de son travail, une augmentation peut être demandée avec une justification du besoin. Les TIC pourraient avoir à facturer les coûts de l'augmentation de quota à l'avenir, mais pour le moment, il n'y a pas de coût additionnel.

Toute demande de quota additionnel devrait être soumise par le superviseur immédiat de la personne. Celui-ci doit confirmer que, dans le cadre de son travail, la personne en question doit avoir accès à d'importants volumes de courriels. La demande doit être faite, par écrit, au directeur des TIC. Toute augmentation de limite, ainsi que la durée de l'arrangement, sera à la discrétion des TIC.