

Charte informatique

OBJET : UTILISATION DE L'OUTIL INFORMATIQUE, MOYENS DE COMMUNICATION ELECTRONIQUES EN RESEAU INTERNE ET EXTERNE AU SEIN DE LA COMMUNE DE MOLENBEEK-SAINT-JEAN

Généralités

L'utilisation des ressources informatiques et en particulier mais non uniquement, des réseaux comme Internet, est une nécessité pour chaque enseignant. A la fois pour des raisons pédagogiques et administratives, chaque membre du personnel enseignant a recours aux facilités que les ressources informatiques procurent.

Le Pouvoir organisateur entend permettre l'accès de tous ses membres à ces facilités dans le cadre des besoins liés aux fonctions qu'ils occupent, et leur exprime ainsi la confiance qu'il leur accorde.

Ainsi, en ce qui concerne le contrôle de l'utilisation de l'outil informatique mis à disposition par le Pouvoir organisateur, les enseignants respecteront les prescrits de la loi du 8-12-1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Au travers des principes déontologiques que le présent document exprime, le Pouvoir organisateur entend rendre conscients ses enseignants des responsabilités qui leur incombent, tant comme utilisateur que comme acteur de telles ressources et des réseaux informatiques.

L'utilisation de ce matériel par l'enseignant qui en dispose se fait dans le cadre de l'exercice de la fonction.

Toutefois, l'utilisation privée de cette technologie est tolérée pour autant qu'elle ne soit pas abusive et ne nuise en rien ni à l'accomplissement du travail, ni au fonctionnement ou à la sécurité du système informatique.

La tolérance s'applique uniquement en dehors des heures normales de service.

Les présentes instructions sont applicables à l'ensemble du personnel enseignant. Elles constituent une annexe au règlement de travail.

Leur violation peut donner lieu à l'application des procédures et sanctions définies en vertu de la législation en vigueur et le règlement de travail du Pouvoir organisateur.

L'utilisation de cette technologie, que ce soit à titre professionnel ou à titre privé, est en outre soumise aux principes repris dans la présente Charte.

ARTICLE 1 - DEFINITIONS

Le présent document définit la position du Pouvoir organisateur à propos:

- de l'utilisation par le personnel enseignant des moyens de communication électroniques en réseau (accès à Internet, utilisation des courriers électroniques, ...);
- de la surveillance des données de communication en réseau (relatives au courrier électronique, à l'accès à internet, ...), et du respect de la vie privée de celui-ci;

Par « outil informatique », on entend tout composant matériel ou logiciel d'un poste de travail desservi au moyen d'un ordinateur personnel ou multiutilisateurs, relié ou non au réseau, en ce compris les matériels d'impression et de communication et leurs périphériques ainsi que tout moyen technique informatique ou bureautique mis en œuvre et visant une meilleure automatisation du travail;

Par "données de communication en réseau", on entend les données relatives aux communications électroniques transitant par réseau tant interne qu'externe, entendues au sens large et indépendamment du support par lequel elles sont transmises ou reçues par un enseignant dans le cadre de la relation de travail.

Article 2 - DEVOIR DE DISCRETION

Il est formellement interdit aux enseignants de divulguer ou d'utiliser directement ou indirectement, à leur profit personnel ou non, qu'ils soient directement ou indirectement obtenus :

- les banques de données et logiciels informatiques;
- les fichiers d'adresses (collègues, élèves, parents, ...);
- les listes de présences ;
- les données personnelles des membres du personnel et de tiers ;
- les informations confidentielles.

L'enseignant doit respecter le secret professionnel tant au cours de sa fonction qu'après la cessation de celle-ci.

Article 3 - SECURITE, ANOMALIES DE FONCTIONNEMENT ET VIRUS

Chaque enseignant est responsable de l'usage personnel des moyens informatiques mis à sa disposition et utilise le système informatique mis à sa disposition en bon père de famille.

La sécurité en matière informatique est une chose complexe qui requiert le bon sens de tous. Afin d'éviter au maximum tout risque de contamination, chaque enseignant doit respecter les règles reprises dans la présente Charte.

Seuls les informaticiens du Service Informatique communal, les fournisseurs et les personnes internes à l'école désignées à cette fin par le Collège des Bourgmestre et Echevins, ont l'autorisation d'installer, de démonter, de déplacer ou de transformer le matériel informatique demandé par les établissements.

Le matériel informatique ne peut être abandonné en état actif ; les sessions actives des programmes utilisés doivent être clôturées par le membre du personnel qui quitte son poste.

Le cas échéant, le matériel informatique doit être mis sous clé. En cas d'anomalie ou de mauvais fonctionnement, l'enseignant doit toujours en référer à sa direction qui fera appel au Service informatique.

De même, les faiblesses éventuelles au niveau de la sécurité du matériel informatique devront être signalées au Service informatique via la direction de l'école.

Il est interdit aux enseignants ne disposant pas de la compétence appropriée de tester la sécurité des systèmes.

L'utilisation de matériel informatique et de programmes sans contrôle préalable de la présence de virus est interdite.

Toutes les clés USB, CD-Rom et autres accessoires doivent notamment faire l'objet d'un contrôle avant leur ouverture. Dans l'hypothèse où un virus est détecté, l'enseignant en avise immédiatement le Service informatique via sa direction. Il ne tente pas de le détruire lui-même.

L'enseignant participe aussi à la non-prolifération de virus en détruisant systématiquement avant ouverture des pièces jointes tout mail qu'il reçoit et qui présente le risque de contenir un virus, comme par exemple :

- des mails d'origine inconnue
- des mails en langue étrangère non utilisée habituellement en Belgique (sauf si l'expéditeur est connu, réputé sans risque et utilise habituellement cette langue)
- des mails qui proposent des gains quelconques moyennant l'une ou l'autre action
- des mails qui invitent leur destinataire à le transférer vers d'autres destinataires (chaînes)
- de manière générale, tout autre mail qui lui paraît douteux.

Tout piratage ou toute tentative de piratage du réseau est interdite.

ARTICLE 4. – SÉCURITÉ ET INSTRUCTIONS EN MATIÈRE D'UTILISATION

4.1. Quant à l'utilisation du courrier électronique

Dans le cadre de leurs relations professionnelles, les enseignants sont tenus d'utiliser exclusivement leur adresse électronique professionnelle.

L'utilisation de systèmes de courrier électronique, tels que email via internet ou via les systèmes de mail internes n'est autorisée que dans le cadre de la fonction.

Lors de l'utilisation de systèmes de courrier électronique, l'enseignant doit savoir que les règles en vigueur relatives au traitement de l'information sont également d'application. En outre, l'enseignant doit être conscient du fait que l'utilisation de systèmes de courrier électronique n'est pas de nature à assurer pleinement la confidentialité.

Pour l'envoi de courrier électronique, les enseignants doivent se servir d'un langage correct et doivent suivre les mêmes règles et normes de politesses que celles applicables à la communication téléphonique et écrite.

Des appels lancés au départ d'internet en vue de diffuser au sein de l'administration communale ou de l'école, des photos, du courrier ou d'autres reproductions par voie électronique, doivent être détruits, même si l'appel semble être sans danger ou sympathique, sauf approbation ou instruction dérogatoire du secrétaire communal.

Les enseignants ne peuvent prendre des engagements qui pourraient nuire d'une quelconque manière à l'administration communale ou à l'école. En outre, ils ne peuvent s'engager (par exemple par des commandes ou ordres) s'ils n'y sont autorisés.

L'enseignant enverra ou recevra des mails personnels par le biais d'une boîte personnelle hébergée sur un serveur externe de messagerie.

Les mails envoyés de ou reçus à l'adresse x@molenbeek.irisnet.be ou toute autre adresse mise à disposition de l'enseignant par l'administration sont présumés être de nature professionnelle. L'administration se réserve donc le droit de consulter ces mails en cas d'absence de l'enseignant.

Si un enseignant souhaite éviter qu'en son absence, un mail sortant soit, le cas échéant, consulté, il doit indiquer clairement la mention PERSONNEL dans l'objet du mail.

L'administrateur réseau (ou son/ses suppléants) est la seule personne habilitée à consulter les mails présumés professionnels d'un membre du personnel, avant communication au collègue qui doit les traiter. S'il est amené à consulter un mail adressé au travailleur sans qu'apparaisse la mention PERSONNEL en objet alors que le contenu de ce mail est personnel, il le requalifiera en mail personnel.

L'administrateur réseau ou l'employeur pourra consulter les mails ou les données de communication lorsque :

- la loi permet ou impose leur interception ou leur prise de connaissance ;
- l'interception ou la prise de connaissance est accomplie dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution du service de télécommunication ;
- lorsque l'état de nécessité peut être invoqué ;
- lorsque tous les participants à une communication ont donné leur consentement.

En aucun cas, le courrier électronique ne pourra être utilisé à l'une des fins prohibées décrites au point 4.6 ci-après. En cas d'utilisation non autorisée du courrier électronique, le Pouvoir organisateur ne pourra être tenu pour responsable du contenu des messages envoyés ou reçus par l'enseignant.

4.2. Quant à l'utilisation d'internet

Le Pouvoir organisateur fournit à ses enseignants l'accès à internet à des fins professionnelles.

Toutefois, l'exploration d'internet dans une optique d'apprentissage et de développement personnel est acceptée, mais ne peut en rien porter atteinte au bon fonctionnement du réseau ou à la productivité de l'enseignant.

La plupart des sites internet conservent une trace des consultations. Certains identifient la provenance du visiteur et son identité électronique, donc celle de l'administration communale.

Est interdit, sans que la liste soit limitative, la consultation :

- de sites à caractère pornographique,
- de sites racistes,
- de sites prônant la discrimination sur base du sexe, de l'orientation sexuelle, du handicap, de la religion ou des convictions politiques d'une personne ou d'un groupe de personnes,
- de sites de casinos,
- de sites qui, de manière générale, engendrent l'utilisation d'internet dans le cadre d'une activité illégale ou commerciale.

Lorsqu'ils parcourent l'internet, les enseignants doivent respecter les dispositions visées au point 4.6 ci-après.

Le Pouvoir organisateur n'assume aucune responsabilité à l'égard de ses enseignants en ce qui concerne les sites visités et le contenu de ceux-ci.

Le Pouvoir organisateur se réserve le droit de bloquer à tout moment et sans avertissement préalable l'accès à certains sites ou type de fichiers dont il juge le contenu illégal, offensant ou inapproprié.

4.3. Quant à l'utilisation de fichiers électroniques

L'enseignant qui souhaite sauver des fichiers personnels doit le faire sur son disque dur (C ou D) sous un répertoire intitulé PERSONNEL. Le format, le nombre et la taille de ces fichiers ne peuvent engendrer de perturbations sur le réseau informatique.

La sauvegarde ou le téléchargement de tout fichier ayant une extension différente de .doc, .xls, .pdf, .ppt de même que de fichiers « exécutables » ou « zippés » est interdit, sous réserve de l'autorisation de la direction ou du secrétaire communal.

L'intervention du service informatique est alors requise.

L'enseignant veillera en outre à respecter toutes les réglementations en vigueur, et notamment celles sur les droits d'auteur.

4.4. L'utilisation de mots de passe, codes d'accès et autres

L'enseignant doit veiller à ce que les mots de passe, codes d'accès et autres moyens de contrôle d'accès soient utilisés de manière strictement confidentielle. Si la confidentialité d'un mot de passe n'est plus garantie, celui-ci doit être modifié.

Dans des circonstances exceptionnelles, ces données doivent être communiquées ou remises sur ordre de leur direction ou du Secrétaire communal, et ce afin de permettre d'assurer la continuité des activités.

4.5. Quant à l'utilisation de logiciels

Seules les versions autorisées de programmes remises par le service informatique ou par les fournisseurs approuvés par ce service (exemple : logiciels commandes de livres fournis par la FWB) , peuvent être utilisées sur les ordinateurs.

Il est interdit de copier ou de télécharger des logiciels, des programmes ou des banques de données. Si un enseignant estime avoir besoin d'un logiciel ou autre produit informatique dans l'exercice de sa fonction, il en réfère à sa direction.

Il est interdit de mettre à la disposition de tiers ou de copier ou télécharger les programmes pris en licence par l'administration, sauf accord écrit et préalable du Secrétaire communal.

4.6. Quant aux activités prohibées

Considérant que le matériel informatique est la propriété du Pouvoir organisateur, que sa responsabilité peut être engagée du fait de l'usage qui en serait fait par ses enseignants et qu'il est nécessaire d'assurer le bon fonctionnement de l'infrastructure informatique du Pouvoir organisateur, il est interdit d'utiliser des moyens de communication électroniques en réseau notamment en vue de:

- la diffusion ou le téléchargement de données protégées par les droits d'auteur, en violation des lois protégeant les droits d'auteur;
- la retransmission de messages électroniques en l'absence de but professionnel légitime, dans des circonstances de nature à porter préjudice au Pouvoir organisateur ou à l'auteur du message originel;
- l'envoi de messages ou la consultation de sites de jeux ou de sites internet dont le contenu est susceptible de porter atteinte à la dignité d'autrui, notamment l'envoi de messages ou la consultation de sites racistes, révisionnistes, érotiques ou pornographiques, de même que les sites prônant la discrimination sur base du sexe, de l'orientation sexuelle, du handicap, de la religion, des convictions philosophiques ou politiques d'une personne ou d'un groupe de personnes;
- la diffusion d'informations confidentielles relatives au Pouvoir organisateur, à ses partenaires ou aux enseignants, sauf dans le cadre strict de la conduite des dossiers du Pouvoir organisateur;
- l'utilisation des systèmes de communication en réseau (e-mail, internet, ...) dans le cadre d'une activité professionnelle ou politique étrangère à la relation de travail liant l'enseignement au Pouvoir organisateur ;
- la commande de biens et services destinés à la vie privée (biens de consommation, placements boursiers, etc.);
- la participation, au départ de l'infrastructure du Pouvoir organisateur, à un "forum de discussion" ou "newsgroup", qui ne soit pas professionnel;
- l'envoi et/ou, en cas de réception, l'ouverture de fichiers exécutables (.EXE), en raison de la menace sérieuse qu'ils constituent pour la stabilité et la sécurité du réseau du Pouvoir organisateur (virus, etc.), de même que le téléchargement de programmes, sauf dans les cas où l'exercice de la fonction le requiert;
- la participation à des "chaînes de lettres", "pyramides" et procédés analogues;
- plus généralement, l'utilisation des moyens de communication électroniques en réseau dans le cadre d'une activité illégale, quelle qu'elle soit.

ARTICLE 5 - SURVEILLANCE DES DONNEES DE COMMUNICATION EN RESEAU ET PROTECTION DE LA VIE PRIVEE DES ENSEIGNANTS

Le matériel informatique est propriété du Pouvoir organisateur.

Le Pouvoir organisateur est fortement attachée au principe du respect de la vie privée de ses enseignants sur le lieu de travail et respecte par conséquent les principes contenus dans la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

Lorsqu'il effectue un contrôle des données de communication en réseau, le Pouvoir organisateur s'engage à le réaliser dans le respect des principes de finalité, de proportionnalité et de transparence tels que prévus dans cette loi.

Le contrôle des données de communication électroniques en réseau ne peut se réaliser que pour autant que l'une ou plusieurs des finalités suivantes est ou sont poursuivies:

- la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau du Pouvoir organisateur, ainsi que la protection physique des installations du Pouvoir organisateur ;
- la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui;
- le respect de bonne foi des principes et règles d'utilisation des technologies en réseau tels que fixés dans le présent document;
- la protection de la réputation, des intérêts économiques et financiers du Pouvoir organisateur.

Le contrôle des données de communication ne peut entraîner une ingérence dans la vie privée du travailleur ou tout au moins qu'une ingérence réduite au minimum.

Ainsi, ne seront collectées en vue du contrôle que les données de communication électroniques en réseau qui sont nécessaires, indispensables au contrôle et qui ont un caractère adéquat, pertinent et non excessif par rapport aux finalités poursuivies.

Les modalités du contrôle sont portées à la connaissance de tous et se font, conformément aux règles applicables en vertu la législation en vigueur.

Pratiquement, en matière de contrôle, l'administration prend un certain nombre de mesures afin :

- de prévenir ou de constater des faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;
- de protéger les intérêts de l'école et de l'administration communale ;
- de garantir la sécurité et le bon fonctionnement des systèmes informatiques, en ce compris le contrôle des coûts et la protection physique des installations mises à disposition ;
- de s'assurer du respect de bonne foi des principes et règles d'utilisation des technologies de l'information et de la communication.

Ces mesures n'empêchent en rien l'enseignant de s'imposer la discipline requise dans l'utilisation des technologies de la communication et de l'information.

Dans le cadre de ces contrôles, l'administration communale respecte la vie privée des enseignants ainsi que les autres réglementations en vigueur.

Un logiciel de filtrage de l'accès aux sites est mis en place.

Un système de contrôle des pièces jointes aux mails ou des fichiers téléchargés est mis en place.

Un contrôle ponctuel et aléatoire est exercé sur le type de sites consultés, le nombre de pages consultées, le temps global de connexion, le nombre de mails reçus ou envoyés, la taille et la nature des pièces jointes ainsi que toute autre donnée rencontrant la finalité recherchée.

En cas de constatation d'abus dans l'utilisation de l'outil informatique, le membre du personnel en cause peut immédiatement être identifié par l'administrateur réseau si l'abus concerne l'un des 3 premiers objectifs visés à cette section. La procédure ci-après décrite s'applique.

L'enseignant concerné est entendu par l'employeur. Le cas échéant, il est averti par l'employeur, par écrit par lettre recommandée ou contre la signature de sa main d'un accusé de réception, qu'un contrôle individualisé le concernant a lieu.

L'analyse des données résultant du contrôle est effectuée par l'administrateur réseau en présence du membre du personnel et, à la demande de ce dernier, d'une personne de son choix (un représentant du personnel, par exemple). Les données recueillies sont consignées dans un procès-verbal par l'administrateur réseau et sont communiquées à l'employeur.

Un second entretien entre le membre du personnel et l'employeur a lieu avant toute sanction éventuelle.

Lorsque la constatation d'abus dans l'utilisation de l'outil informatique a trait au quatrième objectif visé à cette section, une communication est faite au personnel qu'une anomalie de ce type a été constatée et qu'en cas de nouvelle anomalie de même nature, les données de communication seront individualisées.

Le membre du personnel éventuellement individualisé est entendu par l'employeur avant qu'une sanction puisse être prise. Les données permettant le contrôle sont conservées pendant une période de 6 mois sur le serveur.

La protection de la vie privée n'est plus assurée lorsque l'état de nécessité peut être invoqué, c'est-à-dire lorsque certains comportements pénalement sanctionnables sont observés (consultation de sites pédophiles ou terroristes, envoi de mails à caractère xénophobe,...).

Article 6 - SANCTIONS

Tout manquement aux dispositions du présent chapitre peut entraîner le retrait du matériel permettant l'utilisation des technologies de l'information et de la communication.

Il peut en outre entraîner une des sanctions prévues au Règlement de travail.

L'administration communale se réserve le droit de réclamer, le cas échéant, des dommages et intérêts.

Toute sanction prise le sera dans le respect de la proportionnalité au manquement ou à l'infraction.

Article 7 - RESPONSABILITES

Conformément à la législation en vigueur, le membre du personnel, statutaire ou contractuel, répond, en cas de dommages causés par lui dans l'exercice de sa fonction à la personne publique ou à des tiers, de son dol et de sa faute lourde ainsi que de sa faute légère si celle-ci présente dans son chef un caractère habituel plutôt qu'accidentel.

A contrario, ce n'est que dans le cas d'une faute légère ayant un caractère accidentel que le membre du personnel n'engage pas sa responsabilité.

Un « disclaimer » spécifique accompagne tout mail envoyé par le biais d'une adresse nominative. Il précise que le contenu du mail envoyé liant l'administration communale n'a aucune valeur légale, seul un courrier ordinaire faisant foi.

Article 8 – DROIT A LA DECONNEXION

L'utilisation des outils numériques ne peut porter atteinte au respect des temps de repos et de congés ainsi qu'à l'équilibre entre le travail et la vie privée.

Pour les organisations syndicales :

CSC-ENSEIGNEMENT

CGSP-ENSEIGNEMENT

SLFP-Enseignement