VILLE DE
SCEAUX
À LA CROISÉE DES TALENTS

Informatique : guide du bon usage

Annexe n° 12 du règlement intérieur général

Préambule

Dans le cadre de leurs fonctions, les agents ont accès au système d'information de la Ville par l'intermédiaire d'outils informatiques, matériels et logiciels.

Afin de satisfaire au bon fonctionnement entre les services et pour les usagers de la ville de Sceaux, ce système d'information doit être le plus opérationnel possible, et le respect d'un certain nombre de règles contribuera à garantir la qualité du service public délivrée par les services de la Ville.

Le contenu de ce code de conduite informatique a été validé par le comité de pilotage informatique, instance regroupant les directions de services utilisateurs, le service informatique, et le consultant informatique mandaté, sous la direction du directeur général des services. Il a été approuvé au CTP du 22 juin 2006

Partie 1 : Règlement informatique

Article 1 : Matériel

1.1. Aucun matériel informatique, quel qu'il soit, ne peut être emprunté, prêté, échangé, déconnecté ou déplacé de bureau ou de prise sans l'accord du directeur général des services ou du service informatique.

1.2. Les démontages, remontages physiques du matériel informatique sont interdits.

1.3. Il est interdit de débrancher les câbles des réseaux informatiques situés dans les armoires de brassage.

Article 2 : Logiciels

2.1. Il est interdit de copier ou de détourner tout ou partie des logiciels mis à la disposition des collaborateurs, quel qu'en soit le motif. Toute copie peut faire l'objet de sanctions disciplinaires et expose l'agent à des poursuites judiciaires.

2.2. Il est interdit de télécharger des logiciels sans autorisation du service informatique.

2.3. Il est interdit d'installer un logiciel, quel qu'il soit, sans autorisation du service informatique. Tout programme non qualifié et référencé par le service informatique sera supprimé.

2.4. L'apparence de l'interface des logiciels peut-être personnalisée, s'ils le permettent. Tout changement entraînant un dysfonctionnement du système, ou gênant la manipulation (cas des ordinateurs en commun) est interdit.

2.5. Il est interdit de stocker les données de l'utilisateur dans les espaces réservés aux programmes.

2.6. Il est interdit de déplacer, renommer, effacer, désinstaller ou copier les logiciels qui sont installés dans les répertoires ou dossiers.

2.7. Il est interdit de télécharger des écrans de veille et de les installer sur son poste. Seuls ceux déjà disponibles sur les ordinateurs peuvent être installés.

2.8. L'installation de logiciels shareware (logiciels payants à durée limitée : exemple Winzip), et de logiciels peer-to-peer (logiciels ou fichiers mis en communs par les internautes sur des serveurs

permettant notamment le téléchargement de contenus tels que des films, musiques) est interdite sur les postes de travail.

2.9. Il est interdit d'utiliser des logiciels de messagerie instantanée (MSN, ICQ…)

2.10. Il est interdit d'utiliser une autre messagerie que celle mise à disposition des collaborateurs.

Article 3 : Données

3.1. Il est interdit de faire mention de critères raciaux, religieux, syndicaux ou politiques dans les données concernant des personnes physiques, en conformité avec la loi « informatique et liberté ».

3.2. Il est interdit de diffuser à l'extérieur des documents ou fichiers qui contiennent des informations qui ne soient pas de nature publique, sans l'approbation du directeur général des services.

3.3. Il est interdit de déplacer et renommer les répertoires du dossier commun ainsi que les documents produits par autrui sans autorisation du service informatique.

Article 4 : Réseaux

4.1. Il est interdit de télécharger, recopier sur les ordinateurs, graver ou faire usage, même en dehors des heures de travail, des données telles que photos, images ou musique, soumis à la réglementation des droits d'auteur.

4.2. Il est interdit d'écouter radio, musique, télévision…sur le réseau, afin de garantir la vitesse de transmissions des données professionnelles et de ne pas pénaliser les agents dans leur travail.

4.3. Il est interdit de télécharger des programmes, pour lesquels la ville ne possède pas de licences d'utilisation (voir § 2.1).

4.4. Le dispositif de sécurité interdit aux utilisateurs de recevoir par la messagerie des programmes d'exécution (.exe) sans autorisation du service informatique.

4.5. La connexion à des sites Internet à caractère pornographique, terroriste ou violent, est interdite et n'est plus disponible avec la mise en place d'un système de sécurité.

4.6. Une relative tolérance est accordée concernant l'accès à des sites dits de « loisirs », c'est-à-dire ne rentrant pas dans le cadre de l'activité professionnelle de l'agent et non bloqués, dès lors que cela n'entraîne aucune perturbation du travail au regard en particulier, de la durée et de la fréquence des connexions. Tout abus engage la responsabilité de l'agent utilisateur.

4.7. Des contrôles pourront être mis en place par le service informatique à la demande du directeur général des services.

4.8. Il est interdit d'envoyer des messages à caractère racial, antisémite, terroriste, insultant, sur Internet ou à partir de la messagerie interne.

4.9. Il est interdit de tenter de pirater un réseau, un site extérieur à partir d'un poste de la collectivité.

Partie 2 : Guide de bon usage de l'informatique

1) Pour une utilisation optimale du matériel informatique

Chaque agent a la charge d'entretenir son matériel et d'en prendre soin. Ainsi l'entretien externe (dépoussiérage, traces de doigts sur les écrans), doit s'effectuer avec des produits adéquats par l'utilisateur tels que produits spécialisés, chiffons secs. Les services de ménage ne sont pas autorisés à assurer l'entretien des matériels informatiques.

Il convient, afin d'éviter de détériorer le matériel, de ne pas installer de plantations et tout contenant risquant de répandre des liquides en se renversant (eau, café, sodas etc.…). De la même manière, toutes secousses ou vibrations doivent être évitées autour ou sur les postes de travail. Il convient aussi de ne pas déplacer de façon violente le matériel informatique et les périphériques.

Les utilisateurs doivent prendre garde à ne pas obstruer les grilles d'aération du matériel informatique, périphériques inclus, par des feuilles, dossiers, boites ou autres, ce qui produit un échauffement des composants installés à l'intérieur des appareils et les détruit.

Afin de travailler dans de bonnes conditions et de préserver sa santé, il est recommandé de veiller à l'ergonomie de son poste de travail (dos droit, nuque droite, respect d'une distance par rapport à l'écran >50cm et < 70cm, orientation de l'écran évitant les reflets lumineux.)

Le service de médecine professionnelle et préventive est là pour conseiller les collaborateurs de la Ville sur le sujet.

2) Les logiciels mis à la disposition des collaborateurs

Plusieurs types de logiciels sont installés sur les ordinateurs des agents. Ils peuvent être utilisés à volonté, ils font partie des outils de travail. Ce sont essentiellement des logiciels bureautiques (traitement de texte, tableur…), de gestion pour des applications particulières au domaine d'activité des agents (comptabilité, élections, état-civil, ressources humaines etc…), et le système d'exploitation de la machine.
En cas de dysfonctionnements, prévenir dans ce cas le service informatique qui fera remonter le problème à la société éditrice ou prestataire chargée de leur maintenance.

Avec l'accord du service informatique, les agents de la Ville peuvent également développer des bases de données, en respectant les règles de la Commission Nationale Informatique et Liberté mentionnées en partie 1, article 3-1, consultables sur son site Internet : www.cnil.fr (par exemple : pas d'informations contenues, dans les bases de données, à caractère racial, politique, religieux…) Les collaborateurs sont invités à informer les personnes concernées s'ils entrent dans la base des données nominatives.

3) Les données

Dans le cadre de leurs activités, les agents enregistrent des informations et produisent divers documents. Chacun est responsable de ses productions. Les documents émis doivent cependant répondre à la charte graphique mise en place par le service communication. Ces modèles sont disponibles dans le répertoire commun.

Il est possible d'utiliser des données enregistrées dans des fichiers déjà existants pour en extraire des informations qui seront ensuite retraitées pour obtenir un autre résultat.
Les données traitées en entrée et en sortie peuvent prendre diverses formes : texte, images, son.

Les données appartiennent à la collectivité en tant que personne morale et ne sont pas la propriété d'une personne physique. Elles alimentent l'ensemble du système d'informations, et peuvent être confidentielles, réservées ou publiques. Il est donc important d'en laisser l'accès à ses collègues en cas d'absence, pour que le travail puisse être traité malgré tout, et de prévoir avec la direction ou le chef de service une organisation de classement des documents confidentiels du service afin qu'ils ne puissent pas être lus par tous.

Pour cela, les agents ont à leur disposition la possibilité de classer les documents dans des répertoires accessibles à toute la collectivité pour les documents communs (T:\Comm) et dans des répertoires accessibles seulement par le service pour les documents confidentiels.
Tout document, fichier doit être sauvegardé. En effet, en cas de panne du disque dur ou autres raisons, un document ou fichier non sauvegardé serait définitivement perdu, pouvant entraîner des conséquences graves pour la collectivité. Il est donc demandé aux agents d'enregistrer leurs données sur un autre support que celui de leur disque dur.

Tout document, fichier nécessite une sauvegarde selon les procédures suivantes :

Solution 1 à privilégier : enregistrement sur le serveur dont les données sont sauvegardées toutes les nuits et dont les bandes sont rangées dans un coffre ignifugé. La collectivité change de bandes tous les jours ce qui implique que restent toujours 5 jeux de sauvegarde (du lundi au vendredi).

Solution 2 : enregistrement sur un support informatique autre que le serveur: disquettes, CD (les agents ne disposant pas de graveur peuvent demander assistance au service informatique). Ces supports doivent être rangés dans un coffre ou armoire ignifugé.

En cours de saisie d'un document, les collaborateurs doivent enregistrer régulièrement leur travail : en effet en cas de coupure ou micro-coupure de courant, celui-ci serait perdu.

Afin de ne pas surcharger le serveur, il est convenu que chaque utilisateur doit copier les documents anciens, ou qui ne seront plus utilisés avant longtemps dans des répertoires nommées : « A GRAVER », afin que le service informatique puisse les graver sur CD-ROM (si vous ne disposez pas de graveur), et les effacer du serveur. Ces CD seront rendus au service et pourront être classés au service des archives.

Enfin, il est demandé aux utilisateurs de ne pas enregistrer des fichiers sur les postes de travail ou sur les serveurs en plusieurs exemplaires, (principalement les fichiers volumineux), afin de ne pas surcharger l'espace de stockage. Si le cas s'avérait indispensable, demander au service informatique de le graver sur CD.

En cas de destruction de données, les collaborateurs doivent prévenir immédiatement le service informatique, sans essayer d'autres manipulations pour tenter de les récupérer.

4) L'accès aux réseaux

Les collaborateurs peuvent utiliser le réseau de la mairie qui permet de relier entre eux les équipements informatiques et de mettre en commun les ressources physiques et logicielles, avec un accès rapide à tout type d'informations nécessaires dans le cadre du travail.

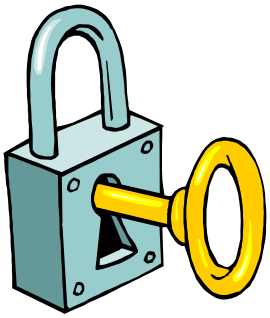
L'accès à un réseau est soumis à l'identification de l'utilisateur par un code utilisateur et un mot de passe.

A travers le réseau local, ils auront accès à un espace réservé aux applications, un espace pour les documents de leur service et un espace pour les documents communs de l'ensemble des services.

Il convient de rester vigilant concernant la réception de documents via Internet, porteurs éventuels de virus informatiques. En cas de doute prévenir le service informatique.

5) La sécurité

L'ensemble des outils informatiques et la masse des informations véhiculée obligent à une attention particulière quant à leur protection. En tant qu'utilisateur, les agents sont concernés par cet aspect, soit pour leur propre sécurité (appareils électriques), soit pour la protection des informations de la collectivité, soit encore pour leur confidentialité.



Le dispositif de sécurité de la Ville (pare-feu et Proxy) permet de filtrer les accès à Internet entrants et sortants, ainsi que les mails circulants sur la messagerie. Des logiciels antivirus sont déployés sur tous les postes de travail ainsi que sur les serveurs.

Ce dispositif empêche d'une part l'accessibilité aux sites pornographiques, terroristes, de violence, et d'autre part l'intrusion sur le réseau de la Ville de tout type de virus, de scripts malveillants et de cookies (fichier espion placé à l'occasion de la consultation d'un site sur le disque dur de l'utilisateur. Il permet de recueillir des données sur le comportement de navigation de l'utilisateur). Il limite les affichages de fenêtres publicitaires.

Le dispositif de sécurité vérifie le contenu des mails entrants et sortants afin de détecter s'ils contiennent des virus. Dans ce cas, les mails sont mis en quarantaine et seront supprimés. Le service informatique a la possibilité de contrôler et d'avoir une vue sur la destination et le contenu des mails. Ceux-ci ne seront lus que si le dispositif de sécurité donne une alerte sur un virus.

L'accès aux matériels, pendant l'absence de chaque collaborateur doit être prévu par l'organisation du service : gestion des clés de portes d'entrée, d'armoires, tiroirs.
En cas d'absence du service, ranger les micros portables dans un lieu fermant à clé.

L'accès au réseau, logiciels, données d'un poste momentanément libre, ne doit pas permettre une intrusion sur le réseau. Avant de s'absenter, il faut fermer les applications en cours d'utilisation et verrouiller son poste de travail (CTL+ALT+SUPPR en appuyant sur ces 3 touches en même temps, pour déverrouiller refaire la manipulation CTL+ALT+SUPPR puis entrer son mot de passe).

Les mots de passe doivent être réservés aux seules personnes pour lesquelles le chef de service souhaite qu'elles aient accès aux informations de l'utilisateur du poste. En cas de doute, les agents doivent prévenir le service

informatique qui changera le mot de passe. De même, en cas de départ d'un agent de la collectivité, il est nécessaire de prévenir le service informatique, qui détruira l'ancien mot de passe et en créera un nouveau pour le nouvel arrivant.

Il est rappelé ici la nécessité d'enregistrer son travail sur le serveur (sauvegarde toutes les nuits), et de sauvegarder sur support informatique tout document qui serait enregistré sur le disque dur.

Afin de ne pas perdre les informations contenus sur les supports de sauvegarde, il est nécessaire de ne pas les laisser près d'une source de chaleur, ni de les tordre, ni les marquer au moyen de stylos billes, stylos-feutres ni de graver au moyen d'outils durs des informations dessus.

En cas de perte ou de vols de matériel ou support informatique, les agents doivent prévenir aussitôt, le service informatique et la direction générale.

Tout incident anormal du fonctionnement de l'équipement informatique (bruits, odeurs, coupures, dysfonctionnements logiciels …) doit être signalé au service informatique.

6) La formation

Formation informatique

La formation informatique sur les logiciels d'application est souvent liée à l'acquisition de nouveaux progiciels ou à des mise à jour de ceux-ci. Il est recommandé aux agents d'être présents lors des prises de rendez-vous des ces formations pour garantir une bonne efficacité dans le travail. Une formation retransmise par un collègue si le collaborateur a été absent pendant celle dispensée par la société fournisseur du progiciel, sera moins efficace.

Formation bureautique

La formation bureautique est dispensée en interne par le service informatique en collaboration avec le service des ressources humaines, et s'étale tout au long de l'année. Le service des ressources humaines propose un calendrier et les thèmes abordés pendant ces formations et se charges des inscriptions. Pour tout besoin de formation, les agents sont invités à contacter la Direction des Ressources Humaines.