07/09/2015

Charte de bon usage de l'informatique, des réseaux et du téléphone

Applicable aux agents de l'ensemble des Services de l'USTOM du Castillonnais et du Réolais

Sommaire

Préambule

Objet

La présente charte rappelle les règles d'utilisation des moyens informatiques et téléphoniques de la collectivité afin de favoriser un usage optimal de ces ressources en termes de sécurité, de confidentialité, de performance, de respect de la règlementation et des personnes.

Champs d'application

La présente charte s'applique à tous les agents de la collectivité, quel que soit leur statut, leur fonction et leur ancienneté (y compris les agents occasionnels ou saisonniers), aux élus, stagiaires, visiteurs, et plus généralement à l'ensemble des personnes utilisant les moyens informatiques et téléphoniques de la collectivité.

Communication

Dès son entrée en vigueur, la charte sera mise à disposition à une place convenable et accessible à tous dans tous les services. Elle est annexée au Règlement Intérieur de la Collectivité.

Application et révision

Cette charte est soumise pour avis au Comité technique (CT), ainsi que toutes modifications ultérieures par voie d'avenant.

L'autorité territoriale, ainsi que toute personne ayant autorité, sera chargée de son application. En cas de non-respect de ces dispositions, les agents pourront se voir infliger des sanctions disciplinaires.

Bases légales

Le présent paragraphe a pour objectif d'informer les utilisateurs des principaux textes législatifs et règlementaires définissant notamment les droits et obligations des personnes utilisant les moyens informatiques. Il ne s'agit en aucune manière d'une liste exhaustive.

- Loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, imposant notamment les obligations de réserve, de discrétion et de secret professionnel des agents publics.
- Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverse dispositions d'ordre administratif, social et fiscal.
- Loi n°78-71 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés qui a notamment pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique et d'encadrer l'utilisation des données à caractère personnel dans les traitements informatiques.
- Loi du 3 juillet 1985 et la directive de la CEE du 21 décembre 1988 qui interdisent à l'utilisateur d'un logiciel toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.
- Loi du 5 janvier 1988 sur la fraude informatique.
- Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.
- Code pénal, pris notamment en ses articles 323-1 à 323-7 visant les atteintes aux systèmes de traitement automatisé des données.
- Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
- L'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Article 1 – Accès aux ressources informatiques, service internet/intranet et moyens téléphoniques

1-1 : Utilisation des ressources

Les ressources informatiques, l'usage des services internet/intranet et du réseau pour y accéder, ainsi que les moyens téléphoniques, sont mis à disposition des utilisateurs, tels que définis dans le préambule de la présente charte, pour l'exercice des activités de la collectivité, voire des prestations demandées par la collectivité à ses prestataires, même occasionnels (ex : stagiaires).

Toutefois, il est admis qu'un usage raisonnable des ressources à des fins personnelles peut être toléré, à la condition expresse de respecter les dispositions de la présente charte. Cet usage personnel des ressources ne pourra être qu'occasionnel et limité, dans le temps et par son objet.

Un administrateur réseau est désigné. Il est amené à effectuer diverses opérations techniques pour fournir un service de qualité aux utilisateurs. Ces opérations peuvent conduire l'administrateur à prendre connaissance d'informations de nature confidentielle, et doivent faire ceci en respectant les droits fondamentaux de l'utilisateur (protection des données personnelles, vie privée, secret des correspondances).

1-2 : Documents privés et professionnels

L'utilisateur veillera à distinguer clairement les documents, courriers, message, etc. qu'il considère comme personnels, des documents professionnels, notamment en les rangeant dans des dossiers distincts nommés « privés », et/ou en faisant figurer « privé » en tête du nom du document et de l'objet des courriels.
Tout document ou courriel ne respectant pas cette règle sera considéré comme professionnel.

1-3 : Responsabilité

L'utilisateur est informé de sa propre responsabilité, celle de son chef de service, et la responsabilité de la collectivité peuvent être engagées civilement et pénalement du fait de son comportement. Il veillera donc à respecter les lois et règlements en vigueur ainsi que les règles d'utilisations, de sécurité et de bons usages décrits dans la présente charte.

1-4 : Abus et contrôles

L'utilisateur est informé que tout abus de l'utilisation non professionnelle fera l'objet de sanctions. De ce fait, il reconnaît avoir été averti que le système d'information de la collectivité fait l'objet d'une surveillance constante (serveurs, réseaux, postes de travail, téléphones, logiciel, virus, etc.) et qu'en cas de comportement suspect, certains équipements sont soumis à une surveillance particulières, notamment sur les volumes d'informations traitées (enregistrement, téléchargement), les durées anormales d'utilisation, les connexions à des sites internet prohibés ou les tentatives d'intrusions, par exemple.

Ainsi sont conservées de manière automatique les informations suivantes :

- L'adresse et l'heure de toute connexion à un site web depuis un ordinateur utilisant le réseau de la collectivité,
- Une copie de tout courrier électronique réceptionné et émis par le serveur de messagerie de la collectivité, y compris les courriels non sollicités (SPAM),
- Le numéro appelé, l'heure, la durée et le coût de tous les appels téléphoniques externes passés par les postes téléphoniques et les fax reliés au réseau téléphonique de la collectivité.

La gestion de ces données est faite dans le respect de la Loi Informatique et Libertés.

1-5 : Mesures conservatoires et sanctions

Tout utilisateur ne suivant pas les règles et obligations rappelées dans cette charte pourra se voir, par mesure conservatoire, suspendre l'accès aux ressources informatiques, téléphoniques ou à certains services (internet, messagerie, etc.).

En cas de manquement grave et d'intention manifeste de nuire au bon fonctionnement des ressources ou à l'activité des services, il sera passible de sanctions disciplinaires proportionnelles à la gravité des manquements constatés.
Tout utilisateur n'ayant pas respecté les lois pourra être poursuivi civilement et/ou pénalement.

1-6 : Prise de main et observation à distance

Le service informatique des différents prestataires dispose d'outils de prise en main à distance qui sont généralement employés pour dépanner les utilisateurs. Ces prises de main et observations à distance doivent toujours se faire avec l'accord de l'intéressé : il est averti par un message sur l'écran qu'il doit valider pour que la prise de main ou l'observation puisse démarrer.

1-7 : Absence de l'agent

En cas d'absence de l'agent, la continuité du service doit être assurée. L'agent doit veiller à ce que le service puisse accéder aux documents, logiciels et dossiers indispensables à l'activité (transmission des documents et dossiers aux collègues ou mise à disposition dans un dossier partagé, création de comptes pour accéder aux applications, à l'exclusion de toute communication de mots de passe personnels).
Si l'absence est imprévue (maladie, accident), le supérieur hiérarchique de l'agent pourra demander au prestataire informatique l'accès à l'espace de travail de l'agent.
En cas de départ définitif ou de mutation, le successeur récupère les documents de travail ainsi que les messages d'ordre professionnels, à l'exception des documents et messages privés (cf. article 2).

Article 2 – Règles d'utilisation, de sécurité et de bon usage

Tout utilisateur est responsable du bon usage des équipements mis à sa disposition. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale.
L'utilisation de ces ressources doit être rationnelles et loyales afin d'éviter leur saturation ou leur détournement à des fins personnelles.

En particulier, l'utilisateur doit appliquer les recommandations suivantes :

2-1 : Sécurité des données et du réseau

2.1.1 Mots de passe

Il convient de s'identifier clairement et utiliser des mots de passe pour protéger l'accès à ses matériels et programmes.
Ces mots de passe ne doivent pas être communiqués, ni notés sur des supports accessibles à autrui, ils ne doivent pas être facile à deviner par une personne mal intentionnée (par ex : pas de prénoms ou dates de naissances de proches). Pour des raisons de sécurité la collectivité se réserve le droit d'imposer un changement régulier des mots de passe.
Les mots de passe sont personnels et chaque utilisateur est responsable de l'utilisation qui peut en être faite. L'emploi de mots de passe commun à plusieurs personnes est interdit. Néanmoins, cette disposition ne s'applique pas lorsque les comptes ou les ordinateurs sont liés à une fonction ou à une structure.

2.1.2 Usurpation d'identité

Ne pas tenter de masquer sa véritable identité ou d'usurper l'identité d'une autre personne pour essayer d'accéder à ses informations ou ses traitements.
Les courriels sont notamment protégés par le secret de la correspondance. Nul ne peut en prendre connaissance sans autorisation de l'émetteur ou du destinataire, à l'exception d'un juge d'instruction ou d'un officier de police judiciaire, qui peut, en cas de plainte, procéder à la saisie des données nécessaires à la manifestation de la vérité.
Il convient de signaler à l'autorité territoriale toute tentative d'accès anormale à son poste de travail et, de façon générale, toute anomalie que l'on peut constater.

2.1.3 Données d'autrui

Ne pas tenter de lire, copier ou détruire des données autres que les siennes. En particulier, ne pas modifier de fichiers contenant des informations comptables ou d'identification, ni tenter de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées, exception faite des données diffusées dans des dossiers publics ou partagés qui sont clairement identifiés.
Il est expressément rappelé qu'accéder sans autorisation à des informations d'autres utilisateurs, les copier, les divulguer, les modifier ou les effacer, peut être sanctionné pénalement.
L'administrateur réseau de la Collectivité est soumis aux mêmes règles, concernant les données d'autrui, que les autres agents de la collectivité.

2.1.4 Informations confidentielles

Ne pas divulguer des informations confidentielles, notamment par téléphone, à des tiers qui ne doivent pas les connaître.

2.1.5 Accès aux postes de travail

Ne pas laisser des ressources ou services accessibles à des tiers en cas d'absence du poste de travail. Mettre l'ordinateur en veille ou verrouiller le poste avant de s'absenter, même momentanément.
La mise en fonction automatique de l'économiseur d'écran, au bout de quelques minutes d'inactivité, est vivement recommandée avec saisie obligatoire d'un mot de passe pour quitter la veille.
Restreindre l'accès aux locaux accueillant les traitements sensibles, notamment ceux soumis à la déclaration à la CNIL. Veiller à ce que les impressions ou sauvegardes contenant des informations sensibles ou nominatives ne soient pas accessibles à des personnes non autorisées (ex : conservation sous clé).
Egalement tout support (papier, cd-rom, etc.) doit être rendu illisible avant mise au rebut.

2.1.6 Téléchargement et installation de logiciels

Ne pas télécharger, installer, utiliser ou contourner les restrictions d'utilisation d'un logiciel pour lequel la collectivité n'a pas acquis de licence. Seul le prestataire informatique est habilité à installer des logiciels, y compris des logiciels libres. Tous les logiciels doivent faire l'objet d'une demande officielle d'installation au prestataire informatique qui en définira les modalités.

Ne pas copier un logiciel pour l'utiliser sur un autre poste ou en dehors de son lieu de travail.

2.1.7 Equipements étrangers

Ne pas connecter sans autorisation, à un poste ou au réseau, un équipement étranger à la collectivité (disques durs externes, modem, clé USB, etc.) et susceptibles de provoquer des dysfonctionnements ou d'introduire des virus informatiques.
Toute connexion d'un nouveau matériel doit se faire avec l'autorisation préalable de l'informaticien.

2.1.8 Messagerie

Ne pas ouvrir de pièce jointe d'un courriel dont on n'est pas absolument certain de la provenance et de l'innocuité. Si cette pièce jointe est un document contenant des macros (tels que Word ou Excel), ne pas permettre l'exécution de ces macros dans ce cas. Il est possible que des actions préjudiciables soient effectuées par ces macros (macrovirus).
La messagerie dispose d'un outil de filtrage qui élimine automatiquement tout message suspect, en entrée et en sortie. La sélection est faite sur le type et le nom des pièces jointes. Sont également éliminés tous les messages considérés comme des « pourriels » (spam) et qui sont reconnus par la teneur du titre ou du texte du message. Attention ces filtres ne sont pas fiables à 100%. Certains pourriels ne sont pas détectés et il peut aussi arriver qu'un message vous étant destiné ait été éliminé.
L'utilisation à titre professionnel, de comptes de messagerie non gérés par la collectivité est interdite.

Remarque importante :
Un message électronique peut constituer une preuve et peut engager fermement son expéditeur et son destinataire. Toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent donc à la messagerie. L'envoi de messages électroniques doit respecter les mêmes procédures de contrôle, de validation et d'autorisation que les courriers.
Il est souhaitable de mettre systématiquement en copie des messages importants son chef de service ainsi que celui du destinataire, et il obligatoire de transmettre pour validation à votre chef de service tout message qui aurait valeur contractuelle ou d'engagement.
Par ailleurs, tout message important doit être conservé à des fins d'archivage.

2.1.9 Virus

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux, que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites connus.
Des comportements inhabituels d'un logiciel ou d'un ordinateur tels que l'ouverture de fenêtre intempestives, l'activité inexpliquée du disque dur ou la dégradation importante des performances peuvent traduire la présence d'un logiciel parasite : contacter rapidement le service informatique.

2.1.10 Antivirus

Il est installé sur les ordinateurs un logiciel destiné à les protéger des programmes malveillants. Cet outil ne doit pas être désinstallé et il est paramétré pour se mettre à jour régulièrement (reconnaissance de nouveau virus). Le paramétrage ne doit donc pas être modifié. Il est recommandé aux utilisateurs d'ordinateur portable de se connecter régulièrement au réseau informatique pour que cette mise à jour puisse être effectuée.
Attention, en cas de détections de virus, un message du logiciel antivirus vous avertit : contacter immédiatement le service informatique.

Article 2-2 : Règles minimales de courtoisie et de respect d'autrui

Il convient de faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques.

2.2.1 Opinions personnelles et propos illicites

Ne pas émettre d'opinions personnelles étrangères à son activité professionnelle et susceptibles de porter préjudice à la collectivité. Sont notamment interdits la consultation, la rédaction, le téléchargement, l'enregistrement, l'envoi et la diffusion de messages, textes, images, films, pages web, etc. à caractère injurieux, raciste, discriminatoire, insultant, dénigrant, diffamatoire, dégradant, pornographique, faisant l'apologie de crime, incitant à la haine.
De même, les propos susceptibles de révéler les opinions politiques, religieuses, philosophiques, les mœurs, la santé des personnes ou encore porter atteinte à leur vie privée ou à leur dignité, ainsi que les messages portant atteinte à l'image, la réputation ou la considération de la collectivité sont à proscrire.

Remarque :
Un agent ne peut être tenu pour responsable s'il reçoit de tels documents sans les avoir sollicités.

2.2.2 Envoi des messages

Veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter l'encombrement inutile de la messagerie et une dégradation des temps de réponse.