Envoyé en préfecture le 25/09/2019
Reçu en préfecture le 25/09/2019
Affiché le 22/05/2019
ID : 091-219102860-20190923-DEL_2019_0109-DE

Charte informatique Ville de GRIGNY

1. Objet du document

La ville de GRIGNY met à la disposition de ses utilisateurs des équipements informatiques (serveurs, PC, tablettes, smartphones, logiciels…), des moyens de communication (réseaux intersites, messagerie, accès Internet…), ainsi que des données et informations qui sont nécessaires à l'accomplissement de leurs missions.
Chaque utilisateur doit être conscient que l'usage de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi, de la sécurité de la commune et d'un code de bonne conduite.

Dans ce cadre, le présent document a pour objet de préciser les droits, obligations et responsabilités de la collectivité et des utilisateurs.

2. A qui s'applique la charte :

Tout utilisateur régulier ou occasionnel, quel que soit son statut (élu, agent titulaire, contractuel, intérimaire ou stagiaire, étudiant, consultant…) est soumis à la présente Charte Informatique.
Elle engage également la collectivité sur les moyens mis à disposition des utilisateurs.

3. Conditions d'utilisation :

Tout utilisateur s'engage à n'utiliser les moyens informatiques mis à sa disposition que dans le cadre exclusif de son activité au sein de la collectivité et donc à titre professionnel.
Tout utilisateur n'a accès qu'aux informations qui lui sont nécessaires dans le cadre de son activité, ces informations peuvent être propres (ex : documents de l'utilisateur), partagées ou à diffusion interne ou publique.

L'agent doit veiller à ce qu'il soit possible d'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**).

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable et présente un intérêt au regard des fonctions exercées ou des missions à mener.

Une consultation très ponctuelle, pour un motif personnel, des sites Internet dont le contenu est conforme à l'ordre public, aux bonnes mœurs et ne met pas en cause l'intérêt et la réputation de la collectivité, est tolérée, en particulier en dehors du temps de travail de l'agent.

L'adresse de messagerie professionnelle doit être le vecteur privilégié d'échange, à l'exclusion de toute adresse de messagerie privée.

Un usage très raisonnable de la messagerie, dans le cadre des nécessités de la vie courante et familiale, est toléré, à condition que cela n'affecte pas le trafic normal des messages professionnels.
L'envoi en masse à titre privé est interdit.
Un utilisateur qui utilise sa messagerie professionnelle à titre privé doit identifier l'objet de ses mails personnels comme étant privés. En l'absence de précisions, le message sera par défaut considéré comme étant professionnel.

Il en est de même pour les documents personnels, à défaut de la mention « données personnelles » ceux-ci seront considérés comme professionnels.

4. Responsabilité et engagements de l'utilisateur :

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques mises à sa disposition par la collectivité.

L'utilisateur est tenu à l'obligation de discrétion professionnelle pour les données et informations auxquelles il a accès dans le cadre de ses activités professionnelles.

Il s'engage au respect des lois et notamment aux règles relatives :

- À la protection de la vie privée ;
- Au respect de la propriété littéraire et artistique (respect des droits d'auteurs) ;
- À l'interdiction de messages de nature diffamatoire, injurieux, discriminatoire, religieux, d'incitation à la violence, à caractère raciste, pornographique, etc…
- À la confidentialité des données nominatives. La constitution de fichiers informatiques comportant des données nominatives, régie par les dispositions du Règlement Général pour la Protection des Données, est soumise à autorisation préalable auprès du Délégué à la Protection des Données. Compte tenu de l'aspect public d'Internet, le transfert de données nominatives vers l'extérieur est strictement interdit sauf autorisation du Délégué à la Protection des Données.

Il s'engage à ne pas perturber volontairement le fonctionnement du système d'information de la collectivité et notamment à :

- Ne pas interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés ;
- Ne pas introduire des programmes virus ;
- Ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, ou saturer les ressources ;
- Ne pas modifier les configurations des matériels ;
- Ne pas installer ou désinstaller de logiciels sur ces matériels ;
- Ne pas déplacer les matériels sans l'aval de la DSIT;
- Ne pas visualiser des vidéos ou écouter de la musique ou la radio depuis des sites internet externes, sans raison professionnelle.
- Etc…

Les périphériques de stockage des postes de travail (exemple : clé USB, disque dur externe, etc..,) sont tolérés, sous réserve que l'utilisateur en garantisse une provenance fiable. Il est ainsi interdit de raccorder des clés USB inconnues, trouvées, offertes dans des salons, etc., sans vérification préalable de leur innocuité.
La clé USB est un vecteur utilisé pour le piratage des postes de travail. Une clé peut s'infecter lors d'une utilisation sur un matériel contaminé (une machine commune destinée aux présentations par exemple).
De la même façon, la connexion de disques externes, téléphones portables, GPS,…. non maîtrisés expose au même danger.

La connexion des terminaux personnels privés de type ordinateur portable, smartphone, tablette, etc. au réseau de la collectivité est interdite.

5. Absence ou départ de l'agent :

En cas d'absence de l'agent, la continuité du service auquel il est affecté comme d'un autre service de la collectivité, doit être assurée.

Si l'absence est imprévue (maladie, accident), le supérieur hiérarchique pourra demander au service informatique l'accès à l'espace de travail de l'agent à l'exception des « données personnelles » (*Voir paragraphe 3*)

En cas de départ définitif ou de mutation, le successeur récupère les documents de travail ainsi que les messages d'ordre professionnel,

Lors de son départ de la collectivité, l'utilisateur doit remettre à sa hiérarchie, en bon état de fonctionnement, l'ensemble des moyens informatiques et de communication électronique mis à sa disposition dans le cadre de ses fonctions (ordinateur, périphériques, mobile, tablette, badges, supports de stockage…).

Les codes d'accès aux systèmes d'information et à la messagerie seront désactivés ou supprimés au départ de l'agent.
Les répertoires ou documents identifiés « données personnelles » seront supprimés par l'utilisateur la veille de son départ de la collectivité. A défaut et sauf procédure judiciaire ou enquête administrative, ce répertoire sera supprimé par le service informatique, sans être consulté et sans qu'aucune copie ne soit réalisée.

6. Dispositions relatives à l'envoi en masse de courriels

En cas de nécessité de diffusion à l'ensemble de la collectivité, l'utilisateur devra :

- Obtenir l'aval par mail de la Directrice Générale des Services ou de la Directrice Générale Adjointe des Finances ou du Directeur Général Adjoint Ressources
- Transférer cette validation au service informatique (dsi.reseau@grigny91.fr)
- Appuyer cette demande par un appel téléphonique en cas d'urgence

7. Mails

Afin de faciliter le travail de tous, il est recommandé de respecter les règles de bon usage de la messagerie suivantes:

- L'objet doit être explicite et clair
- Le texte doit être bref, structuré et aéré
- Le ou les destinataire(s) en original est(sont) celui(ceux) qui fait(font).
- Ne pas abuser des destinataires en copie, n'y positionner que ceux qui ont besoin de l'information.
- Il convient d'être courtois : « bonjour », « cordialement »…
- Ne pas utiliser les mails pour régler des conflits.

Tout utilisateur des équipements informatiques de la ville doit adopter les mesures de prudence visant à les protéger d'attaque malveillante. Il doit en particulier :

- Porter une attention aux expéditeurs inconnus
- Se méfier des demandes étranges, toujours se poser la question de la légitimité des demandes éventuelles exprimées. L'adresse de messagerie source n'est pas un critère fiable.
- Aucun organisme ne demandera par e-mail de lui communiquer des informations personnelles.
- Vérifier les liens dans le courriel : avant de cliquer sur les éventuels liens, laisser sa souris dessus. Apparaît alors le lien complet. S'assurer que ce lien est cohérent et pointe vers un site légitime.

S'il y un doute sur un message reçu, il y a de fortes chances que celui-ci ne soit pas légitime. Il convient alors de ne surtout pas ouvrir les pièces jointes, de ne pas y répondre et de contacter le service informatique pour l'en informer.

8. Réseaux Sociaux

L'utilisation des réseaux sociaux peut être source de risques et de responsabilité notamment en terme d'image.
Dans le cadre de la sphère professionnelle, l'utilisateur doit obtenir l'autorisation de l'autorité territoriale pour pouvoir participer à un réseau social et/ou créer un espace sur un réseau social.
Dans le cadre de la sphère non professionnelle, les utilisateurs sont bien évidemment libres d'utiliser les réseaux sociaux en respectant toutefois les obligations de réserve et de discrétion professionnelle inhérentes au statut d'agent communal.

9. Sécurité, Identifiant, mot de passe :

Les droits et autorisations d'accès aux ressources et logiciels (identifiant + mot de passe provisoire) sont attribués nominativement par le service informatique sur la base des demandes effectuées par les responsables de service.
Le mot de passe provisoire devra être changé, à la première utilisation, par un mot de passe complexe et renouvelé régulièrement.

L'utilisateur est personnellement responsable de l'utilisation qui peut en être faite et ne doit en aucun cas les communiquer. Il doit veiller à ne jamais quitter un ordinateur sans avoir fermé sa session Windows ou l'application utilisée.

En cas de perte ou de vol de matériel professionnel ou privé, afin d'éviter l'utilisation frauduleuse de ses identifiants et mots de passe, l'utilisateur veillera à ne pas les enregistrer sur les navigateurs internet.

Dans le cas d'une tentative de violation ou d'anomalie relative à une utilisation de ses codes d'accès personnels, l'utilisateur doit en informer immédiatement le service informatique.

10. Sécurisation du matériel

Quel que soit l'endroit où il se trouve, l'utilisateur doit veiller à ne pas laisser ses matériels (ordinateur personnel, smartphone, tablette, etc.) en dehors de sa surveillance.
L'utilisation du câble antivol remis avec l'ordinateur portable est obligatoire et constitue une protection efficace pour une absence occasionnelle,

Les utilisateurs auxquels sont confiés des téléphones portables et/ou tablettes dans le cadre de l'exécution de leurs fonctions doivent toujours en conserver la garde matérielle et en particulier ne pas prêter le matériel à un tiers.

L'utilisateur s'engage à informer la DSIT dans les plus brefs délais de toute perte ou vol du matériel mis à sa disposition, y compris personnel, si celui-ci contient des données professionnelles.
Il s'engage à fournir à la DSIT une copie de la déclaration de vol.

11. Rôle et responsabilité de la DSIT

Le service informatique interne de la collectivité assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communications.
Les agents de la DSIT disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place :

- Outils de contrôle, de stockage et d'archivage des données et messages ;
- Un système de journalisation des connexions, destiné à identifier et enregistrer toutes les connexions ou tentatives de connexion, avec conservation des données ne pouvant excéder un an ;
- Une traçabilité des actions (consultation, création, modification, suppression) dans les applications métiers mises en œuvre ;
- La possibilité de prise de contrôle à distance des postes de travail pour des dépannages et installations (après accord de l'utilisateur du poste)

Ils ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.
Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

Aucun mot de passe n'est enregistré au service informatique

La collectivité se réserve le droit d'utiliser des logiciels de filtrage afin d'interdire l'accès aux sites Internet dont le contenu lui apparait illicite ou en contradiction avec les objectifs et principes de la présente charte.

L'utilisateur accepte que la collectivité puisse avoir connaissance des informations nécessaires à l'administration du réseau (données de volumétrie, incidents, nature du trafic engendré) et puisse prendre toutes mesures urgentes pour stopper une perturbation du service.

La collectivité est susceptible de recevoir une demande officielle (réquisition judiciaire) lui demandant de fournir les données permettant d'identifier les communications passées (typiquement : l'identification de l'utilisateur, du terminal utilisé, du type et de la durée des communications).
La durée de conservation de ces données est d'un an.

12. Mesures conservatoires et sanctions encourues :

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

13. Principes d'éco-responsabilité :

Afin de limiter l'impact de son activité professionnelle sur l'environnement, chaque utilisateur est invité à adopter les bons comportements suivants au quotidien :

- Eteindre son ordinateur ainsi que l'écran le soir et le weekend.
- Débrancher les chargeurs et transformateurs lorsqu'ils ne sont pas utilisés
- Eteindre son imprimante le soir et le weekend.
- Ne pas imprimer systématiquement les documents informatiques, n'imprimer que si c'est vraiment utile.
- Privilégier le recto-verso pour les impressions et photocopies.
- Privilégier le noir et blanc à la couleur pour les impressions et photocopies.
- (La couleur coûte 10 fois plus cher)
- Privilégier les copieurs aux imprimantes
- Privilégier la messagerie électronique au courrier postal

Informations légales :

- Règlement Général protection des Données (RGDP) :

https://www.cnil.fr/reglement-europeen-protection-donnees
https://www.cnil.fr/sites/default/files/atoms/files/suis-je_concerne_-_les_principes_vd.pdf

- Loi anti-terroristes n° 2006-64 :

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124

- Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000637071&categorieLien=id

- Loi Hadopi :

https://www.service-public.fr/particuliers/vosdroits/F32108

- Relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (LCEN 2011)

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&categorieLien=id

- Article R. 1321-1 du Code du Travail

https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072050&idArticle=LEGIARTI000018483964&dateTexte=&categorieLien=cid

Ce document a reçu l'approbation du CT le : …….

Notifié le :
Signature