Envoyé en préfecture le 17/12/2022
Reçu en préfecture le 17/12/2022
Publié le
ID : 081-218103257-20221215-DELIB_59_2022-DE

CHARTE INFORMATIQUE

I. Préambule

I.1. Le contexte et les enjeux

A l'ère du numérique, les collectivités territoriales sont tenues de prendre en compte l'utilisation croissante des technologies. Ces dernières offrent aux collectivités une ouverture vers le monde extérieur, et leur permettent d'améliorer et de diversifier leurs compétences. L'utilisation de ces outils technologiques doit ainsi être faite de manière consciente, et doit répondre à des règles de bonne conduite.

La transparence et la sécurité sont les principes clés qui doivent être retenus dans le cadre de l'utilisation du numérique. En effet, une mauvaise utilisation des outils numériques peut avoir des conséquences néfastes sur la confidentialité, l'intégrité et la sécurité des données personnelles. Elle peut causer, en outre, une perte de productivité, et l'addition de coûts superflus.

Ainsi, la préservation du système d'information va de pair avec une l'instauration d'une bonne hygiène informatique, en vue d'assurer le bon fonctionnement des services et les droits et libertés de chacun.

I.2. L'objet

La présente charte vise à reprendre l'ensemble des règles nécessaires à la réalisation de ces objectifs. Les règles légales et de sécurité relatives à l'utilisation du/des système(s) d'information et de communication au sein de la commune de Viviers-Lès-Montagnes seront mises en avant dans cette charte. Les droits et les obligations des utilisateurs seront définis.

Le non-respect de ces règles pourra entraîner le retrait du droit d'utilisation de l'outil, de l'application ou du matériel en question. Il pourra s'en suivre de mesures d'ordre disciplinaire, et/ou des poursuites pénales pourront être engagées.

I.3. Le champ d'application

Cette charte s'applique à l'ensemble des moyens de communication et des ressources informatiques et numériques de la collectivité. Elle concerne notamment (cette liste est non exhaustive) :

- Les applications métiers, bureautiques, messagerie, internet, intranet, extranet,
- Données, adresses électroniques, comptes réseaux et sociaux,
- PC fixes et portables, tablettes, périphériques (imprimantes, USB,…)
- Téléphones fixes, portables, fax
- Carte d'accès aux services

La charte s'applique à l'ensemble du personnel, tous statuts confondus. Elle s'applique également au personnel temporaire, ainsi qu'aux prestataires extérieurs ayant accès aux données et outils informatiques de l'établissement. Les contrats avec les prestataires extérieurs devront y faire référence (la charte devra être présentée en annexe).

Les élus sont également soumis au respect de la présente charte.

Chaque agent et élu se verra remettre un exemplaire de la présente charte. Il devra en prendre connaissance, et s'engager à la respecter.

II. Les règles générales d'utilisation

Dans le cadre de l'utilisation des outils numériques présents au sein de la collectivité, les utilisateurs sont présumés adopter un comportement responsable. Ils s'engagent, à ce titre, à prendre en compte les interdictions d'accéder à des données ou à des sites.

Les utilisateurs sont responsables des utilisations qu'ils font des ressources informatiques, ainsi que du contenu qu'il affiche, télécharge ou envoie. Ils s'engagent à ne pas effectuer des opérations qui seraient néfastes ou bloquantes pour le réseau.

A l'instar de l'utilisation des ressources informatiques, le courrier, le téléphone, ou la télécopie sont sous la responsabilité de la personne qui en fait l'usage. Les messages ou les appels envoyés ou reçus sont sous la responsabilité de l'utilisateur concerné. La messagerie doit être utilisée, à ce titre, dans le respect des missions et des fonctions accordées à l'utilisateur concerné.

Les utilisateurs se doivent de garder à l'esprit le fait que l'utilisation du réseau se fait sous le nom de l'institution. L'image renvoyée est donc à prendre en compte. En outre, les règles de courtoisie et de bienséance doivent être respectées.

II.1. Droits et devoirs des utilisateurs

II.1.1. Modalités d'accès aux ressources informatiques et numériques

Tout utilisateur a la charge, autant qu'il le peut, de contribuer à la sécurité générale du système d'information. Ainsi, l'utilisation des ressources doit être rationnelle et loyale : leur détournement à des fins personnelles est strictement proscrit.

Les agents travaillant dans l'établissement disposent d'un droit d'accès au système d'information. Ce droit est strictement personnel et incessible.

L'accès aux ressources informatiques repose sur une authentification de la part de l'utilisateur. La création d'un identifiant (login) doit intervenir dès l'arrivée d'un nouvel utilisateur travaillant au sein de la collectivité. Un mot de passe personnalisé doit y être associé.

Les moyens d'authentification sont strictement personnels et confidentiels. Chaque utilisateur est responsable de l'utilisation qui peut être faite de ses identifiants.

II.1.2. Droits et obligations des utilisateurs et de la collectivité

Les ressources informatiques sont un outil de travail nécessaire à la bonne réalisation des tâches. Chaque utilisateur doit respecter les règles définies ci-dessous :

- L'utilisation des ressources est limitée à l'exercice de l'activité professionnelle, dans le cadre des missions établies par la collectivité
- Ne pas stocker ou transmettre des informations portant atteinte à la dignité humaine
- Respecter les données d'autrui : ne pas tenter de les lire, modifier, copier ou détruire, exception faite aux données présentes dans des dossiers publics ou partagés qui sont clairement identifiés
- Respecter les droits de propriété intellectuelle, à savoir la non-reproduction et/ou la non diffusion de données soumises à un droit de propriété intellectuelle. Cela concerne également le respect des licences d'utilisation de logiciels pour lesquelles seule la collectivité est habilitée
- Ne pas perturber la disponibilité du système d'information (que ce soit par utilisation anormale du système, ou par l'introduction de logiciels non sécurisés, de sources malveillantes, etc.)
- Ne pas introduire de « ressources extérieures » matérielles ou logicielles, ou « équipements étrangers » qui pourraient porter atteinte à la sécurité du système d'information
- Respecter les contraintes liées à la maintenance du système d'information
- L'utilisateur s'engage à ce qu'aucune de ses données identifiées comme étant privées ou personnelles soient stockées sur le serveur. Les données qui y sont conservées doivent être purement professionnelles.
- Les documents personnels stockés sur le poste de travail doivent porter la mention « personnel » ou « privé »

La collectivité s'engage à mettre à disposition les ressources informatiques matérielles et logicielles nécessaires à l'exécution des missions des utilisateurs. Elle s'engage à respecter la confidentialité des « données utilisateurs » auxquelles elle pourrait être amenée à accéder. Elle s'engage à définir les règles d'usage de son système d'information, et veillera à leur application.

Pour veiller à ce que les devoirs et droits des utilisateurs soient respectés, la collectivité peut être en mesure d'effectuer une surveillance du système. Cette surveillance a pour unique but de veiller à ce que le système d'information soit sécurisé. Elle est réalisée conformément à la règlementation en matière de protection des données personnelles.

II.1.3. Gestion des accès

En cas d'absence d'un agent, la continuité du service public doit être assurée. L'agent doit veiller à ce que, en son absence, la collectivité puisse accéder au poste et applicatifs sur lesquels figurent des informations ou des fichiers nécessaires à l'exécution de l'activité.

En cas de départ définitif d'un agent, la continuité du service doit également être assurée. En revanche, il convient de prendre les mesures nécessaires quant à la suppression des anciens accès, et quant à la création de nouveaux accès pour l'agent remplaçant, dans un délai raisonnable. Les données « privées » ou « personnelles » qui auraient pu être conservées sur le poste informatique doivent être supprimées.

II.2. Mesures de sécurité pour l'accès au système et aux applicatifs

L'utilisateur se voit remettre un identifiant et un mot de passe pour accéder au système d'information. Ce mot de passe est personnel, et incessible.

Dans un souci de sécurité globale, la création de mots de passe pour accéder au système d'information ainsi qu'à toutes les plateformes ou logiciels utilisés est requise. Les mots de passe doivent différer selon l'applicatif/logiciel auquel l'utilisateur souhaite se connecter.

Les mots de passe doivent répondre à des exigences de sécurité suffisantes. A ce titre, l'utilisateur s'engage à sécuriser la conservation de ses mots de passe. En outre, les mots de passe choisis doivent comporter un minimum de douze (12) caractères, dont :

- un nombre,
- une majuscule,
- un signe de ponctuation ou un caractère spécial

Les mots de passe doivent être renouvelés à minima tous les six (6) mois. Le responsable en la matière se garde le droit, pour des raisons évidentes, de modifier ce délai en cas de doute sur la sécurité du système.

Envoyé en préfecture le 17/12/2022
Reçu en préfecture le 17/12/2022
Publié le
ID : 081-218103257-20221215-DELIB_59_2022-DE

III. Utilisation des postes informatiques

Un ensemble d'équipements sont mis à disposition de l'utilisateur. Parmi eux :

- Le matériel : unité centrale, écran, clavier, etc.
- Système d'exploitation
- Logiciels

L'utilisateur doit prendre soin des équipements qui sont mis à sa disposition. Une attention particulière doit être portée aux supports amovibles (clés USB, etc.), afin d'éviter d'infecter le poste.

L'installation de logiciels est à la charge de la personne désignée comme étant compétente en la matière.

En cas d'absence momentanée, l'utilisateur veille à ce que son poste soit verrouillé le temps de son absence, afin d'éviter l'intrusion de tiers. En cas d'absence prolongée, l'utilisateur doit quitter/déconnecter les applications et verrouiller son poste. A la fin de sa journée de travail, l'utilisateur doit également se déconnecter des applications, arrêter le système et éteindre l'écran ainsi que l'imprimante.

Des dispositifs de sauvegarde quotidienne des informations doivent être mis en œuvre.

L'utilisateur se doit de signaler tous dysfonctionnements ou anomalies au service compétent ou à la personne référente.

IV. La messagerie

L'utilisation de la messagerie est réservée à des fins professionnelles. Dans le cadre de cette utilisation, l'utilisateur veille à :

- Ne pas ouvrir les mails, pièces jointes, ou liens qui paraissent suspects
- Les courriels à caractère privé et personnel doivent être identifiés comme « privé » dans l'objet du message ou dans le nom du dossier où ils sont stockés
- L'utilisateur respecte les règles de la bienséance et de la courtoisie
- Lorsque l'utilisateur fait un envoi « groupé », il veille, lorsque cela est nécessaire, à ce que les destinataires soient en copie cachée.

V. Logiciels métier et télé-services

Par logiciel métier, sont entendus les logiciels de gestion accessibles en ligne tels que le Système d'information géographique, Logiciel comptable, état civil, HelpDesk, etc.

Envoyé en préfecture le 17/12/2022
Reçu en préfecture le 17/12/2022
Publié le
ID : 081-218103257-20221215-DELIB_59_2022-DE

Chaque utilisateur veille à ce qu'il soit authentifié pour accéder au logiciel. Cette authentification se fait au travers d'un login et d'un mot de passe sécurisé.

L'utilisateur doit respecter les règles d'usage du logiciel métier pour lequel des droits lui ont été attribués.

VI. Internet

L'utilisation d'internet est réservée à des fins professionnelles. Il est néanmoins toléré, en dehors des heures de travail, un usage modéré de l'accès à internet pour des besoins personnels, à condition que cela soit réalisé de manière sécurisée et que cela n'occasionne pas de difficultés quant à l'usage professionnel.

L'utilisateur s'engage à ne pas se rendre sur des sites portant atteinte à la dignité humaine ou n'étant pas conforme, sous aucun prétexte, à un usage raisonnablement attendu dans le milieu professionnel (sites à caractère pornographique, sites faisant l'apologie des crimes contre l'humanité, provocation à la discrimination, etc.)

Le téléchargement de données numériques (musiques, images, logiciels propriétaires, etc.) soumises aux droits d'auteur, ou au copyright, est strictement proscrit.

VII. Téléphone

L'utilisation des téléphones fixes et portables fournis par la collectivité est réservée à des fins professionnelles.

En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service, ou sur l'accueil téléphonique.

VIII. Télétravail

Le télétravail est une forme d'organisation du travail qui permet à l'agent de travailler ailleurs que dans son service ou ses locaux habituels grâce aux technologies de l'information et de la communication. Il est prévu aux articles L1222-9 à L1222-11 du Code du travail.

Tout agent de la fonction publique, fonctionnaire ou contractuel, peut exercer une partie de son activité en télétravail, si cette activité peut être réalisée à distance, aux moyens d'outils informatiques.

Une délibération doit venir fixer les conditions d'exercice du télétravail dans la collectivité. Elle doit notamment prévoir les règles à respecter en matière de sécurité des systèmes

d'information et de protection des données. Les règles énoncées dans la présente charte sont à prendre en compte.

IX. Protection des données personnelles

Dans le cadre de la réglementation en vigueur (Règlement Général sur la Protection des Données à caractère personnel entré en vigueur le 25 mai 2018, et Loi Informatique et Libertés n°78-17 du 6 janvier 1978), la collectivité s'engage à respecter les données personnelles.

La collectivité et l'utilisateur s'engagent pour que les données personnelles soient :

- obtenues et traitées loyalement, licitement et de façon transparente,
- collectées pour des finalités déterminées et licites sur la base de l'intérêt légitime de la ville
- utilisées conformément à ces finalités,
- adéquates, pertinentes et non excessives par rapport à ces finalités dans le respect du principe de minimisation.

Conformément à la règlementation en vigueur, les personnes disposent d'un droit d'accès et de rectification de leurs données personnelles ainsi que de celui d'en demander l'effacement, le droit de s'y opposer à leur traitement et d'en obtenir la limitation ou la portabilité dans la mesure où cela est applicable, sous réserve des motifs légitimes impérieux dont pourrait justifier la collectivité pour conserver ces données.

Le Délégué à la Protection des données de la collectivité est l'Association des maires et des élus locaux du Tarn : *dpd@maires81.asso.fr*

X. Droit à la déconnexion des agents

L'utilisation du numérique est devenue incontournable au travail. La ligne entre le lieu de travail et le lieu de vie personnel s'efface de plus en plus. Il convient donc de mettre en place les protections nécessaires à la santé des salariés.

La « Loi travail » du 8 août 2016 instaure le droit à la déconnexion, qui vise à assurer des temps de repos et de congés, à garantir l'équilibre entre vie professionnelle et vie personnelle et familiale, et protéger la santé des salariés.

- *L'agent n'est pas dans l'obligation de répondre à ses mails en dehors du temps de travail,*
- *L'employeur s'assure régulièrement que la charge de travail pesant sur l'agent est raisonnable*

- *L'employeur fait en sorte, dans la mesure du possible, de ne pas solliciter l'agent en dehors de son temps de travail si cela peut être remis au lendemain,*
- *Etc.*

XI. Sanctions applicables

Les droits et obligations des utilisateurs des ressources informatiques sont définis par la présente Charte, de la loi et des textes réglementaires.

Tout utilisateur ne respectant pas la loi et les règlements en vigueur peut faire l'objet de poursuites pénales.

Tout utilisateur ne respectant pas les règles définies dans la présente Charte est passible de sanctions définies par la collectivité, telles que des sanctions disciplinaires qui seront prises de manière proportionnelle à la gravité des manquements constatés.

XII. Evolution de la Charte

Avant son entrée en vigueur, la présente Charte a été soumise au Conseil Municipal, et a été approuvée à ce titre par délibération. Sa modification est subordonnée à un avis du Conseil Municipal, selon les mêmes formes.

XIII. Dispositions finales

L'accès aux ressources informatiques ne pourra se faire qu'après acceptation des modalités précisées ci-dessus. L'application de la présente Charte pourra faire l'objet de contrôles de la part de l'autorité compétente au sein de la collectivité.

La présente Charte est annexée à tout contrat de travail, de stage, ou de toute autre nature menant à l'utilisation des ressources informatiques.

La présente Charte a été approuvée par délibération du Conseil Municipal.

Le Maire

Alain VEUILLET

Envoyé en préfecture le 17/12/2022
Reçu en préfecture le 17/12/2022
Publié le
ID : 081-218103257-20221215-DELIB_59_2022-DE

XIV. Acceptation de la Charte par l'utilisateur

Je soussigné(e) :

NOM :
……
……

Prénom :
……
….

Service : ……..

Fonction : ……

Utilisateur des ressources informatiques et des outils numériques de la Collectivité……
….., déclare avoir pris connaissance de la présente Charte et m'engage à la respecter.

Fait à ……. Le ……

Signature

Envoyé en préfecture le 17/12/2022
Reçu en préfecture le 17/12/2022
Publié le
ID : 081-218103257-20221215-DELIB_59_2022-DE

ANNEXE : Législation applicable

Chaque agent est responsable de l'utilisation qu'il fait des moyens informatiques. A cette occasion, il peut voir sa responsabilité individuelle engagée du fait de sa mauvaise utilisation.

La présente Annexe a pour objectif d'informer les utilisateurs des principaux textes législatifs et réglementaires en vigueur, qui définissent les droits et les obligations des personnes utilisatrices des ressources informatiques. Cette liste n'a pas vocation à être exhaustive.

- Loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés », relative à l'informatique, aux fichiers et aux libertés, qui a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'informatique, et notamment encadrer l'utilisation des données à caractère personnel conformément au Règlement Général sur la Protection des Données à caractère personnel (RGPD, Règlement (UE) 2016/679)
- Loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires imposant notamment les obligations de réserve, de discrétion et de secret professionnel des agents publics.
- Article 133 de la loi n°2012-347 du 12 mars 2012, permettant le télétravail aux agents publics
- Décret n° 2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature
- Article 226-15 sur l'atteinte au secret des correspondances
- Articles 323-1 à 323-7 du Code pénal relatifs aux atteintes aux systèmes de traitement automatisé de données (fraude informatique)
- Article L112-2 du Code de Propriété Intellectuelle, conférant une protection aux logiciels par le droit d'auteur
- Loi n°2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme