THÔNES
Cœur des Vallées

N° 2024/03

Envoyé en préfecture le 29/03/2024
Reçu en préfecture le 29/03/2024
Publié le 29/03/2024
ID : 074-217402809-20240321-CM24048-DE

EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS DU CONSEIL MUNICIPAL DE THÔNES

SÉANCE DU 21 MARS 2024

L'an deux mil vingt-quatre, le vingt et un du mois de mars, les membres du Conseil Municipal, dûment convoqués en Séance Officielle à dix-neuf heures trente, se sont réunis dans la Salle Consulaire, sous la présidence de M. Pierre BIBOLLET, Maire.

Étaient présents : Mme Michèle FAVRE D'ANNE, M. Claude COLLOMB-PATTON, Mmes Chantal PASSET, Nelly VEYRAT-DUREBEX, M. Stéphane DELÉAGE, Maires-Adjoints,

Mmes Nicole LAURIA, Christine RUFFON, Muriel PÉRILLAT-dit-LEGROS, Brigitte VULLIET, MM. Rodolphe PALACIOS, Stéphane FAURE-HUDRY, Karim CHALABI, Grégory BAERT, Stéphane BESSON, Mme Claire BARRIN, MM. Pierre BASTARD-ROSSET, Richardo RODRIGUES, Michel CATON, Mmes Christine RODRIGUES, Catherine DUTEIL, M. Frédéric VAILLANT, Mme Graziella POURROY SOLARI, M. Rémi FRADIN, Conseillers Municipaux.

Avaient donné procuration : M. Pierre LESTAS, Maire-Adjoint,
M. Sébastien ATRUX-TALLAU, Mme Élisa DE POORTER, M. Benjamin DELOCHE, Conseillers Municipaux.

Était absente : Mme Joëlle TIBURZIO, Conseillère Municipale.

Date de la convocation :	**14 mars 2024**
Nombre de Conseillers Municipaux en exercice :	**29**
Présents et représentés :	**28**

Secrétaire : M. Karim CHALABI, Conseiller Municipal, prend place au bureau en qualité de secrétaire, fonction qu'il déclare accepter.

--==oo0oo==--

N° 2024/048 - CHARTE INFORMATIQUE – ADOPTION

Le développement des technologies de l'information et de la communication conduit le personnel, les élus de la ville et du CCAS à utiliser dans leur travail quotidien l'outil informatique, les réseaux et les services de communication numérique pour l'exécution de leurs missions.

Cette utilisation peut comporter un certain nombre de risques à la fois techniques mais également juridiques pouvant engager la responsabilité de la collectivité et de ses agents.

La charte informatique, jointe en annexe, définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources de la collectivité.

Elle a également pour objet de sensibiliser les utilisateurs aux risques d'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de la collectivité.

Vu le Code Général des Collectivités Territoriales ;

Vu la loi n o 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi sur le règlement général sur la protection des données du 20 juin 2018 ;

Vu l'avis favorable du Comité technique du 22 novembre 2023 ;

../...

Envoyé en préfecture le 29/03/2024
Reçu en préfecture le 29/03/2024
Publié le 29/03/2024
ID : 074-217402809-20240321-CM24048-DE

Considérant que la charte informatique s'applique à l'ensemble du personnel tous statuts confondus ainsi qu'aux élus et qu'elle s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques de la collectivité ;

LE CONSEIL MUNICIPAL, après en avoir délibéré,
Par vote à main levée, à l'unanimité,

- **ADOPTE** la charte informatique telle qu'elle est présentée en annexe.
- **PRÉCISE** que cette charte sera communiquée à chaque agent en poste de la collectivité, à tous les nouveaux arrivants ainsi qu'aux prestataires ayant accès aux données et/ou aux outils informatiques de la collectivité.

AINSI FAIT ET DÉLIBÉRÉ AUX LIEU ET DATE SUSDITS

THÔNES, le 22 mars 2024

Le Maire,

Pierre BIBOLLET

POUR COPIE CONFORME

Le secrétaire de séance

Karim CHALABI

LE MAIRE CERTIFIE LE CARACTÈRE EXÉCUTOIRE DE LA PRÉSENTE DÉLIBÉRATION PAR TÉLÉTRANSMISSION EN PRÉFECTURE DE LA HAUTE-SAVOIE LE 29 MARS 2024 ET PUBLICATION ÉLECTRONIQUE LE .

THÔNES, le

Le Maire,

Pierre BIBOLLET

Envoyé en préfecture le 29/03/2024
Reçu en préfecture le 29/03/2024
Publié le 29/03/2024
ID : 074-217402809-20240321-CM24048-DE

THÔNES
Cœur des Vallées

CHARTE INFORMATIQUE

MAIRIE DE THÔNES – CCAS DE THÔNES

PREAMBULE

La MAIRIE DE THÔNES fournit un système d'information nécessaire à l'exercice de ses missions. Il met ainsi à disposition de ses agents plusieurs outils informatiques.
La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques de la collectivité.
Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite.
L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'institution.
Elle donne un cadre pour définir un comportement responsable et un bon fonctionnement pour tous, en décrivant tous les moyens nécessaires pour contrôler et assurer la protection des personnes et de la collectivité, en fonction des risques encourus par l'agent et l'employeur, ainsi que les contraintes légales.

La présente charte, recueil de règles législatives, réglementaires, de déontologie et de sécurité a pour objet :

- ✓ De définir l'ensemble des bonnes pratiques d'utilisation des ressources informatiques et de communication,
- ✓ De préserver l'intérêt de chacun et l'intérêt général,
- ✓ De préserver un environnement de travail professionnel,
- ✓ De garantir l'intégrité du système informatique,
- ✓ De protéger les informations qui sont la propriété de la collectivité, tout en garantissant l'équilibre de chacun,
- ✓ De limiter les risques de recherche de responsabilités pénales et civiles de chacun.
- ✓ De ce fait, elle s'impose aux personnels de la collectivité, toutes catégories confondues.

Cette charte et ses principes associés s'imposent également aux prestataires et services extérieurs utilisateurs ou ayant simplement accès aux NTIC (nouvelles technologies de l'information et de la communication) de la collectivité.

Après présentation au Comité Technique de la collectivité, la charte fait l'objet d'une note de service qui lui confère un caractère opposable.
Elle est portée à la connaissance de tout agent concerné qui la signe.
La présente charte s'applique à toutes les nouvelles technologies d'information et de communication mises à disposition des agents par l'employeur (ordinateur portable, fourniture d'accès internet, PC, smartphone…) mais également à tout élément en lien avec le service.

Envoyé en préfecture le 29/03/2024
Reçu en préfecture le 29/03/2024
Publié le 29/03/2024
ID : 074-217402809-20240321-CM24048-DE

ARTICLE 1 – RAPPEL REGLEMENTAIRE

La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.

La collectivité, en tant que responsable du traitement, est astreint à une obligation de sécurité. Elle prend les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation à des tiers non autorisés.

La collectivité a désigné un correspondant informatique et libertés (CIL). Ce dernier a pour mission de veiller au respect des dispositions de la loi citée précédemment.
Il est obligatoirement consulté par le responsable des traitements préalablement à leur création. Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de la collectivité au fur et à mesure de leur mise en œuvre.

Le correspondant veille au respect des droits des personnes en matière d'informatique et de données personnelles (droit d'accès, de rectification et d'opposition).
Il élabore chaque année un rapport et un bilan d'activité.

Dans le cadre des NTIC, au même titre que dans l'ensemble de ses activités que ce soit pendant son activité ou en dehors, tout agent de la collectivité est soumis notamment au secret professionnel, à la discrétion professionnelle et à l'obligation de réserve (loi 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires).
Le secret professionnel a pour objet de protéger les intérêts matériels et moraux des particuliers dans la mesure où les agents de la collectivité sont dépositaires de renseignements les concernant.
La discrétion : les fonctionnaires ne peuvent être déliés de cette obligation de discrétion professionnelle que par décision expresse de l'autorité dont ils dépendent. L'obligation de discrétion professionnelle a pour objet de sauvegarder l'intérêt de l'administration.
L'obligation de réserve : la réserve n'a pas trait uniquement à l'expression des opinions. Elle impose au fonctionnaire d'éviter en toutes circonstances les comportements portant atteinte à la considération du service public à l'égard des administrés et des usagers.
L'apparition et l'utilisation des NTIC imposent à chacun de faire preuve de discernement dans ces domaines.
En cas de manquement chaque agent s'expose comme tout citoyen à des sanctions pénales, notamment en cas de :

- Atteinte à la vie privée d'autrui (Cf. articles L.226-1 à 226-5 et L.226-5 à 226-7),
- Diffamation et injure publique et non publique (Cf. loi de 1881 et articles R.624-3 et R.624-4 du CP),
- Provocation de mineurs à commettre des actes illicites ou dangereux, le fait de favoriser la corruption d'un mineur, l'exploitation à caractère pornographique de l'image d'un mineur, la diffusion de messages à caractère violent ou pornographique susceptibles d'être perçus par un mineur (CF. articles sur la mise en péril des mineurs 227-15 à 227-28-1),
- Incitation à la consommation de substances interdites (Cf. article 222-39),
- Provocation aux délits de crimes et délits et la provocation au suicide (Cf. articles 223-13 à 223-15-1), la provocation à la discrimination à la haine notamment raciale, ou à la violence (Cf. article R.625-7),
- Apologie de tous les crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité, la négation de crimes contre l'humanité (Cf. articles 211-1 et suivants, 212-1 et suivants, 213-1 et suivants),

• Contrefaçon, reproduction, représentation ou diffusion d'une œuvre de l'esprit (par exemple : extrait musical, photographie, extrait littéraire…/Cf. articles L.335-5 du Code de la Propriété Intellectuelle) ou d'une prestation de droit voisin (par exemple : interprétation d'une œuvre musicale par un artiste, phonogramme, vidéogramme, programme d'une entreprise de communication audiovisuelle) en violation des droits de l'auteur, du titulaire des droits voisins et/ou du titulaire des droits de propriété intellectuelle (Cf. articles L.335-1 à 10 et 336-1 à 4 du Code de la Propriété Intellectuelle),
• Copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle (Cf. article L.122-6-6). les sanctions pénales sont aggravées pour certaines de ces violations lorsque ces dernières sont commises par un agent public (Cf. article 226-13).

En complément du dispositif pénal, chaque agent ne respectant pas les orientations de cette charte est susceptible de faire l'objet de sanctions disciplinaires.
La collectivité se réserve également la possibilité de restreindre, voire de supprimer, l'accès aux moyens des NTIC, d'un agent dont les pratiques seraient non conformes à cette charte.

ARTICLE 2 – CHAMP D'APPLICATION

La présente charte s'applique à tout utilisateur du système d'information de la collectivité. Le système d'information est composé de l'ensemble des outils informatiques et de communication de la collectivité. Les dispositions de la présente charte sont également applicables aux autres moyens externes connectés au réseau de la collectivité.

Le système d'information est composé des ressources suivantes (liste non exhaustive) :

- ✓ Ordinateurs (fixes et portable)
- ✓ Téléphones (fixes et GSM)
- ✓ Réseau informatique (serveurs, routeurs et connectique)
- ✓ Photocopieurs
- ✓ Imprimantes
- ✓ Logiciels
- ✓ Données informatisées
- ✓ Messagerie
- ✓ Intranet
- ✓ Internet
- ✓ SIRH

ARTICLE 3 – REGLES D'UTILISATION DU SYSTEME D'INFORMATION

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par la collectivité.

1. Principe général de responsabilité et obligation de prudence

L'utilisateur est responsable des ressources informatiques qui lui sont confiées dans le cadre de ses missions, et doit concourir à leur protection, notamment en faisant preuve de prudence. L'utilisateur doit s'assurer d'utiliser les ressources informatiques mises à sa disposition de manière raisonnable, conformément à ses missions.

Envoyé en préfecture le 29/03/2024
Reçu en préfecture le 29/03/2024
Publié le 29/03/2024
ID : 074-217402809-20240321-CM24048-DE

2. Poste de travail.

La collectivité met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions. (Équipement fixe ou nomade).
Chaque poste est configuré en « utilisateur standard » ne permettant pas la modification de la configuration informatique, l'installation ou la suppression de logiciel.
Seul l'administrateur système (compte administrateur) a accès à ces capacités.
Si un agent constate que son poste est configuré en « administrateur système » il doit impérativement le signaler à son responsable hiérarchique ou au référent informatique.

Dans tous les cas l'utilisateur ne doit pas :

- ✓ Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique et/ou logicielle.
- ✓ Connecter ou déconnecter du réseau les outils informatiques sans y avoir été autorisé par le service informatique.
- ✓ Y connecter tout appareil informatique et/ou électronique (clé USB, smartphone etc…) sans y avoir été autorisé par le service informatique.
- ✓ Déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade »).
- ✓ Utiliser cet équipement pour effectuer des actions illégales.

Toutes les données générées dans le cadre de la fonction de l'agent doivent l'être **impérativement et uniquement** dans les répertoires dédiés à cet effet qui sont stockés dans le cloud.

Aucune donnée professionnelle ne doit être stockées en local sur le poste de travail.

Procédures spécifiques aux matériels de prêt

a. Equipements nomades

On entend par « équipements nomades », tous les moyens informatiques mobiles (ordinateurs portables, clés USB, disques durs portables).

Les équipements nomades fournis par la collectivité sont soumis aux règles de la charte.

Une fiche doit être signée par l'utilisateur pour le prêt d'un ordinateur portable ou de tout équipement nomade.

Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements.

L'utilisation de ce matériel est strictement professionnelle et doit respecter les règles de la présente charte.

L'utilisateur doit Informer immédiatement la direction générale des services en cas d'incident sur l'appareil nomade (dysfonction, perte, vol, dégradation…).

3. Login et mot de passe

L'accès aux SI ou aux ressources informatiques mises à disposition est protégé par mot de passe individuel. Ce mot de passe doit être gardé confidentiel par l'utilisateur afin de permettre le contrôle de l'activité de chacun. Le mot de passe doit être mémorisé et ne doit pas être écrit sous quelque forme que ce soit. Il ne doit pas être transmis ou confié à un tiers ou être rendu accessible. Le login et le mot de passe doivent être saisis lors de chaque accès au système d'information.

Le mot de passe doit se conformer à la politique de mot de passe édictée conformément aux prescriptions de la CNIL relativement à la protection des données personnelles et notamment :

- ✓ Être composé d'au moins 12 caractères ;
- ✓ Ces caractères doivent être une combinaison de caractères alphanumériques de chiffres, de majuscules, de minuscules et de caractères spéciaux

Un système de double authentification est également déployé au sein du système d'information pour garantir l'intégrité des accès avec des méthodologies différentes selon les postes : empreinte digitale, reconnaissance faciale ; reconnaissance GSM, code pin etc.

Si la commune met à disposition des utilisateurs un coffre-fort électronique destiné à stocker les mots de passe de manière sécurisé, tous les agents seront soumis à ce dispositif.

Aucun mot de passe ne doit être noté sur papier ou dans un fichier accessible.

L'accès au système d'information avec du matériel n'appartenant pas à l'entreprise (assistants personnels, ordinateur personnel, supports amovibles…), ne peut se faire que sur autorisation expresse de la collectivité et après que le service informatique ait contrôlé et validé le respect du cahier des charges en matière de sécurité informatique.

4. Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations, et en particulier des données personnelles, traitées sur le SI de l'organisation.

IL s'engage à prendre toutes les précautions utiles pour éviter que ne soient divulguées de son fait, ou du fait de personnes dont il a la responsabilité, ces informations confidentielles.

5. Verrouillage de sa session

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

Lorsque l'agent quitte son service (soir, week-end, vacances), sauf exception et sur demande du service informatique, tout le matériel informatique doit être éteint.

6. Logiciels informatiques

L'utilisateur ne doit pas installer, copier, modifier ou détruire de logiciels sur son poste informatique sans l'accord du service informatique en raison notamment du risque de virus informatiques.

Dans le cas ou l'exercice des missions de l'agent nécessite l'installation, la modification ou la suppression d'un logiciel informatique, il doit en faire la demande au référent informatique de la collectivité selon la procédure suivante :

- L'agent doit remplir la demande sur le formulaire de « demande d'installation / modification / suppression de logiciel informatique. »
- Ce formulaire est remis au référent informatique.
- Le référent informatique prend connaissance de la demande, en contrôle la cohérence et donne un avis.
- Le (la) directeur (directrice) général (e) des services valide ou refuse la demande.
- Le référent informatique envois la demande à l'administrateur système qui après la vérification de conformité aux protocoles de sécurité, procèdera à l'installation / modification / suppression du logiciel.

7. Copie de données informatiques

L'utilisateur doit respecter les procédures définies par la collectivité afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité, afin d'éviter la perte de données.

ARTICLE 4 – INTERNET ET MESSAGERIE ELECTRONIQUE

1. Accès à internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le service informatique. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est autorisé, sous réserve d'une validation préalable de la collectivité. Un tel mode d'expression est susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée des utilisateurs est donc indispensable.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de la collectivité, y compris sur Internet.

2. Messagerie électronique – E-mail

La messagerie électronique est un moyen d'amélioration de la communication au sein des entreprises et avec les tiers. Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par la collectivité.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer le service informatique des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

Par principe, tous les messages envoyés ou reçus sont présumés être envoyés à titre professionnel.

Envoyé en préfecture le 29/03/2024
Reçu en préfecture le 29/03/2024
Publié le 29/03/2024
ID : 074-217402809-20240321-CM24048-DE

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

La forme des messages professionnels doit respecter les règles définies par la collectivité notamment en ce qui concerne la mise en forme et la signature des messages.

a. Utilisation personnelle de la messagerie

Par exception, les utilisateurs peuvent utiliser la messagerie à des fins personnelles, dans les limites posées par la loi. Les messages personnels doivent alors porter la mention "PRIVE" dans l'objet et être classés dans un répertoire "PRIVE" dans la messagerie, pour les messages reçus.

Lors de son départ définit de la collectivité l'agent devra procéder à la suppression du système de tous les éléments personnels.

b. Utilisation de la messagerie pour la communication destinée aux institutions représentatives du personnel

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel.

ARTICLE 5 – ADMINISTRATION DU SYSTEME D'INFORMATION

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information de la collectivité, différents dispositifs sont mis en place.

1. Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information et d'assurer la sécurité et la confidentialité des données pourront être mis en œuvre. Il peut s'agir notamment du filtrage des sites internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (peer-to-peer, messagerie instantanée…).

2. Les systèmes de sauvegarde

Un système est en place dans la collectivité permettant de sauvegarder les fichiers de travail présents sur les répertoires, ainsi que les boites mails. Comme indiqué dans l'article 3 - paragraphe 2 – poste de travail – de la présente charte, les données sauvegardées sont celles qui sont stockées sur le cloud. Il est impératif que toutes les données générées par l'agent lors de son travail le soit dans les répertoires dédiées à cet effet. Aucune sauvegarde des données locales (donnée disque dur des postes) n'est effectuée.

3. La gestion du poste de travail

Envoyé en préfecture le 29/03/2024
Reçu en préfecture le 29/03/2024
Publié le 29/03/2024
ID : 074-217402809-20240321-CM24048-DE

Le stockage de fichiers à caractère personnel (par exemple photos personnelles) est toléré sur le disque physique du poste de travail et/ou sur le Drive nominatif du poste, si les volumes occupés restent modestes (de l'ordre de quelques Mo) et s'il ne perturbe pas le bon fonctionnement du poste de travail et/ou du cloud. Les fichiers à caractère personnel seront identifiés comme tel uniquement s'ils sont stockés dans un répertoire clairement identifié « PERSONNEL » ou « PRIVE ».

A des fins de maintenance informatique, la société d'infogérance informatique de la collectivité peut accéder à distance à l'ensemble des postes de travail.
Dans le cadre de mises à jour, évolutions du système d'information ou maintenance, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique des machines. Il s'interdit d'accéder aux contenus sauf nécessité dans le cadre de la continuité du service.

Lorsqu'un contrôle porte sur les fichiers d'un utilisateur et sauf risque ou événement particulier, le service informatique de la collectivité ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur et/ou le cloud qu'en présence de ce dernier et/ou uniquement si celui-ci en a donné l'autorisation.

Relativement à la messagerie électronique ; Le contenu des messages à caractère personnel des utilisateurs, ne peut en aucun cas être contrôlé par le service informatique de la collectivité.

Toute utilisation, stockage ou diffusion d'un logiciel piraté constituent un délit de contrefaçon réprimé par l'article L.335-3 du Code de la propriété intellectuelle (peine pouvant aller jusqu'à 2 ans d'emprisonnement et 152 500 euros d'amendes).

En complément, il est strictement interdit de détenir sur le réseau ou sur tout moyen informatique (y compris smartphone) de la collectivité tout élément à caractère pornographique, sexuel ou raciste.

Enfin, la collectivité n'est en aucun cas garant de la préservation des données non enregistrées sur les supports prévus à cet effet.

L'usage d'une imprimante est destiné à des fins professionnelles. L'usage à des fins personnelles est exceptionnellement admis sur autorisation du responsable hiérarchique.

Lors de son départ définit de la collectivité l'agent devra procéder à la suppression du système de tous les éléments personnels. Dans le cas contraire, tous les éléments restants seront supprimés par l'administrateur du système.

La présente charte comportera éventuellement une annexe technique déterminant les procédures à utiliser pour la connexion et la déconnexion des sessions utilisateurs en toute sécurité.

ARTICLE 5 – MANQUEMENT ET SANCTION

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Envoyé en préfecture le 29/03/2024
Reçu en préfecture le 29/03/2024
Publié le 29/03/2024
ID : 074-217402809-20240321-CM24048-DE

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

ARTICLE 6 : INFORMATION ET ENTREE EN VIGUEUR

La présente charte est ajoutée en annexe du règlement intérieur et communiquée à chaque collaborateur en poste par affichage numérique.

Lors d'embauche elle sera annexée au contrat de travail ou arrêté de recrutement.

Elle entre en vigueur au

Elle a été adoptée après information et consultation du CST le

Fait à ..... *Le*.....