Envoyé en préfecture le 22/11/2024
Reçu en préfecture le 22/11/2024
Publié le
ID : 087-218706505-20241120-2024_D_063-DE

Charte informatique de la commune de Feytiat et de son CCAS et son annexe (Glossaire).

PREAMBULE

Les différents outils technologiques utilisés offrent aux utilisateurs de la commune de FEYTIAT et du CCAS une grande ouverture vers l'extérieur. Cette ouverture peut apporter des améliorations de performances importantes si l'utilisation de ces outils technologiques est faite à bon escient et selon certaines règles. L'usage des moyens numériques mis à disposition doit permettre de préserver le système d'information, le bon fonctionnement des services et les droits et libertés de chacun. L'objectif de la présente charte informatique, document d'information et de référence, est donc de formaliser les règles légales et de sécurité relatives à l'utilisation de tous les outils d'information et de communication au sein de la collectivité.

Une mauvaise utilisation des différents outils technologiques utilisés peut entraîner des conséquences graves : risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité, risque d'atteinte à l'intégrité et à la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vols de données) et du matériel.

Chaque utilisateur doit avoir conscience qu'il a un rôle actif dans ce contexte. Il s'engage à respecter la présente charte.

1. CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à l'ensemble du personnel tous statuts confondus, aux élus et aux utilisateurs du système d'information de la commune de Feytiat et du CCAS. Elle s'applique également

- aux associations utilisant les équipements de la commune ;

- à tout prestataire extérieur ayant accès aux données et aux outils informatiques de la collectivité. Tout contrat avec un prestataire extérieur devra faire référence et comporter comme annexe la présente charte. La charte s'impose de fait à chaque agent œuvrant au sein des services municipaux.

Envoyé en préfecture le 22/11/2024
Reçu en préfecture le 22/11/2024
Publié le
ID : 087-218706505-20241120-2024_D_063-DE

2. POSTES INFORMATIQUES

Toute personne, agent et élu, ou personnes œuvrant dans/pour la collectivité peut disposer d'un droit d'accès au système d'information. Ce droit d'accès est :

✓ **Strictement personnel**
✓ **Incessible.**

Un ensemble « matériels - système d'exploitation – logiciels » est mis à disposition de chaque utilisateur, ce matériel est fragile, il convient d'en prendre soin.
Règles d'usage impératives : Les règles ci-dessous s'imposent à chaque utilisateur :

- En cas d'absence momentanée, l'utilisateur doit verrouiller son ordinateur.
- A la fin de sa journée de travail, l'utilisateur doit fermer les applications et arrêter le système par arrêt logiciel (c'est à cette condition que les mises à jour essentielles sont installées).
- L'utilisateur doit procéder régulièrement à l'élimination des fichiers non utilisés et à l'archivage dans le but de préserver la capacité de mémoire.

D'une manière générale, l'utilisateur doit signaler tous dysfonctionnements ou anomalies à son supérieur hiérarchique.

3. ACCÈS INTERNET ET WIFI

L'utilisation d'Internet est réservée à des fins professionnelles et syndicales dans le cadre de l'exercice des décharges d'activité. Néanmoins, il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.

- Les accès par le WIFI au réseau se fera via l'accès "public", sauf pour les postes référencés et ce quel que soit le matériel (Téléphone, tablette, portable PC/MAC, etc.).

- L'accès par un câble (RJ45) **est interdit** sauf pour les postes référencés.

- L'utilisation du service Wifi est soumise en premier lieu, au respect des lois et des règlements en vigueur.

- L'utilisation de ce service vaut acceptation incontestable par l'utilisateur, sans qu'aucune signature ne soit nécessaire, de l'ensemble des dispositions et obligations contenues dans la présente Charte.

- L'utilisateur reconnaît être dans un lieu ouvert au public. Il s'engage à utiliser tant son matériel informatique, (portable, assistant personnel) et ce service, d'une manière conforme à la loi en s'interdisant notamment tout comportement et tout usage contraire à l'ordre public et aux bonnes mœurs.
En particulier il ne devra pas utiliser son matériel ou ce service à des fins illégales, illicites, interdites, c'est-à-dire, sans que cette liste ait un caractère exhaustif :

• Il s'engage à respecter la loi et s'interdit d'accéder, de mettre en ligne ou d'afficher des contenus et informations, provenant ou non d'une mise en ligne sur le réseau Internet mais considérés comme illégaux par les textes ou les tribunaux tels, les informations, messages, textes, images ou vidéos ayant un caractère violent, d'incitation à la violence ou à la haine, dégradant pour la personne humaine, pornographique ou pédophile et/ou ayant un caractère provocant et portant atteinte à l'intégrité ou à la sensibilité de qui que ce soit.

• L'utilisateur s'engage à respecter la vie privée de toute personne et le secret des correspondances, il s'interdit d'intercepter tout message et communication émis par la voie des télécommunications.

• Il s'engage à respecter la législation sur les données personnelles et les traitements automatisés d'informations nominatives ainsi que la législation et les textes relatifs aux droits d'auteur, marques, brevets, à la propriété intellectuelle et industrielle. Il s'interdit toute reproduction ou usage en infraction de ces législations, qu'il s'agisse de créations multimédia, de logiciels, de textes, d'articles de presse, de photos, de sons, d'images de toute nature, de marques, de brevets, de dessins et modèles, étant précisé que toute mention relative à l'existence de droits sur ces éléments et/ou données et/ou fichiers ne peuvent faire l'objet d'une suppression et que toute reproduction d'une œuvre ou de l'un de ces éléments et/ou fichiers et/ou données sans consentement du titulaire des droits constitue une contrefaçon.
-Dans le cadre de l'usage de ce service, l'utilisateur s'interdit de :

- **Récolter** ou collecter toute information concernant des tiers sans leur consentement ;
- **Diffamer**, diffuser, harceler, traquer, menacer quiconque, ni violer les droits d'autrui ;
- **Créer** une fausse identité ;
- **Tenter** d'obtenir un accès non autorisé à un service et/ou à un fichier, ou une donnée ;
- **Diffuser ou télécharger** des éléments contenant des logiciels ou autres éléments protégés par les droits de propriété intellectuelle, à moins qu'il ne détienne lesdits droits ou qu'il ait reçu toutes les autorisations nécessaires pour le faire ;
- **D'adresser** tout message indésirable ni d'effectuer des envois de type « spamming » ;
- **D'adresser** tout courrier et/ou message électronique comprenant des propos menaçants, injurieux, diffamatoires, obscènes, indécents, illicites ou portant atteinte aux droits des personnes et à la protection des mineurs ;
- **Transmettre** tout virus, cheval de Troie, bombe logique ou tout autre programme nuisible ou destructeur pour les tiers et/ou tout utilisateur ;
- **Tenter** d'obtenir un accès non autorisé à un système automatisé de traitement de données et s'y maintenir ;
- **Perturber** les services et/ou contenus et/ou données auxquels il accède ;
- **D'envoyer** des chaînes de lettres ou proposer des ventes dite « boule de neige » ou pyramidale ;
- **D'adresser** toute publicité, message promotionnel ou tout autre forme de sollicitation ou démarchage non sollicité ;

L'utilisateur reste seul responsable de la sécurité et de la protection de ses équipements connectés. Le fournisseur de service ne peut en aucun cas être tenu de réparer les préjudices directs et/ou indirects subis du fait de l'utilisation du service Wifi par l'utilisateur, ce dernier étant sous la responsabilité des utilisateurs dans le respect de la présente Charte. L'utilisateur reconnaît que le fournisseur de service ne peut être responsable des contenus ou services auxquels il accède et ne garantit ni l'accessibilité aux contenus et services ni la rapidité d'utilisation, l'accès au service Wifi pouvant être suspendu à tout moment sans préavis.

Nous informons les utilisateurs du service que les nouvelles dispositions applicables en matière de lutte contre le terrorisme **impliquent l'obligation de conserver pendant une durée de 12 mois les données techniques de connexion, à savoir : expéditeur, destinataire, heure, durée et lieu d'origine des communications à l'exception de leur contenu**.

Pour éviter les abus, l'Autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes.

4. GESTION DES IDENTIFIANTS ET MOTS DE PASSE

Chaque utilisateur du réseau informatique se voit attribuer un compte auquel sont associés un identifiant (login) et un mot de passe. Il est responsable de l'utilisation qui est faite de ce compte et **il lui appartient donc de ne pas communiquer son mot de passe à une tierce personne**. À cet effet, il ne devra être noté sur aucun support et est, par sa nature, incessible et intransmissible.

5. MESSAGERIE ÉLECTRONIQUE

La messagerie est l'un des premiers vecteurs de propagation des virus et de « phishing » (technique utilisée par des escrocs pour collecter des données personnelles). Il est en effet très simple de diffuser par courriel un fichier attaché contenant un virus ou un lien Internet pour inciter à télécharger un programme infecté.

Au même titre que pour le courrier papier ou le téléphone, chacun est responsable des messages envoyés ou reçus et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues et des règles élémentaires de courtoisie et de bienséance.
Un message envoyé par Internet peut potentiellement être intercepté, même illégalement, et lu par n'importe qui.

Utilisation privée de la messagerie : L'utilisation de la messagerie est réservée à des fins professionnelles.

Néanmoins il est toléré en dehors des heures de travail *un usage modéré* de celle-ci pour des besoins personnels et ponctuels. **Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'Autorité Territoriale (même en l'absence de l'utilisateur).** Ainsi, pour assurer la continuité du service public, l'administrateur informatique, sur demande de l'autorité territoriale peut accéder à la messagerie d'un utilisateur absent en respectant la législation en vigueur et sous certaines conditions : *il est notamment interdit à quiconque de prendre connaissance d'un message professionnel ayant pour objet « Personnel » ou « Confidentiel », sans l'autorisation expresse de l'utilisateur (qu'il en soit l'auteur ou le destinataire).*

Règles d'usage :

- L'utilisateur veillera à ne pas ouvrir les mails dont le sujet paraîtrait suspect (pièces jointes, liens, …).
- Une analyse des pièces jointes est effectuée en temps réel à l'ouverture d'un document envoyé par mail. L'antivirus va bloquer la pièce jointe en cas de suspicion de programme malveillant, mais attention, certains peuvent passer entre les mailles du filet.
- L'utilisateur s'engage à ne pas envoyer en dehors des services de la collectivité des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel et autorisé par son supérieur hiérarchique.
- L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.
- L'utilisateur doit vérifier la liste des destinataires et respecter les circuits de l'organisation ou la voie hiérarchique le cas échéant.
- L'utilisateur doit vérifier le contenu et l'historique des messages transférés.
- L'utilisateur doit éviter de surcharger le réseau d'informations inutiles.

Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être nettoyé périodiquement.

- L'utilisateur utilisera au minimum la fonction répondre à tous.
- En cas d'absence, l'utilisateur devra mettre en place un message automatique indiquant la date de retour prévue et l'interlocuteur auquel s'adresser en son absence.
- Une équivalence juridique est établie entre le courrier électronique et le courrier sur support papier. Ils doivent, en conséquence, être traités dans les mêmes délais.

6. SIGNATURE ÉLECTRONIQUE ET CERTIFICAT

Certains utilisateurs, dans le cadre de leurs fonctions, sont amenés à utiliser des certificats de signature électronique pour signer des documents et/ou s'authentifier pour accéder à des services sécurisés. Ces certificats sont nominatifs et non cessibles, ils sont constitués de 3 éléments indissociables :

- Les informations concernant l'identité du titulaire, son organisation, sa fonction, la période de validité du certificat et l'identité de l'autorité de certification qui l'a généré,
- La clé privée,
- La clé publique.

L'utilisateur doit ainsi veiller à garder confidentiel le code à saisir (clé privée) lors de la signature avec son certificat. Les certificats ont une durée de validité limitée.

Toutes les demandes de certificat ou de renouvellement devront être validés par l'autorité territoriale. Les certificats seront révoqués lorsque leur utilisateur quitte la collectivité ou ne dispose plus de l'habilitation à l'utiliser.

7. PARE-FEU / ANTI-VIRUS

Le pare-feu vérifie tout le trafic de la collectivité, aussi bien local que distant. Il détient toutes les traces de l'activité qui transite par lui s'agissant :

- De la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels)
  La liste des activités de connexions est conservée un mois.
- Des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe. **Un mail supprimé est conservé 30 jours dans la corbeille**.

Il filtre notamment les URL des sites non autorisés par le principe de la liste noire.

8. TÉLÉPHONES ET TABLETTES PROFESSIONNELS

L'utilisation des téléphones fixes et portables est réservée à des fins professionnelles. Néanmoins, un usage ponctuel du téléphone pour des communications personnelles locales est toléré à condition que cela n'entrave pas l'activité professionnelle. **L'Autorité territoriale peut procéder au contrôle de l'ensemble des appels et messages émis et reçus**.

En cas d'absence, l'utilisateur doit :

- Effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique ;
- Ou laisser un message d'absence sur la messagerie téléphonique portable ;
- Ou verrouiller sa messagerie téléphonique sur son portable ;
- Le smartphone/tablette est un outil de travail dont l'usage personnel peut être autorisé (mention "personnel" pour messages personnels) ;
- Il n'est pas obligatoire de répondre aux appels ou aux mails en dehors du temps de travail (soir, week-end et congés sauf astreinte) ;
- Le smartphone/tablette ne doit pas venir perturber une réunion ou un entretien qui nécessitent la présence physique et intellectuelle de chacun.

9. ACCÈS À DISTANCE ET NOMADISME

Le développement du nomadisme et du télétravail ne cesse de prendre de l'ampleur ces dernières années et il est aujourd'hui au centre des réflexions. L'emploi d'ordinateurs portables, de smartphones ou de tablettes facilite le transport et l'échange de données. Circuler avec ces appareils nomades fait cependant peser des menaces sur des informations sensibles dont le vol ou la perte entraîneraient des conséquences importantes sur les activités de l'organisation.

Les équipements d'accès à distance peuvent être mis à disposition pour un usage strictement professionnel et ne doivent en aucun cas être utilisés par des personnes ne faisant pas partie de la collectivité et/ou n'ayant pas signé la présente charte.

Lorsque ces matériels sont utilisés à l'extérieur, notamment dans le cadre de réunion ou d'intervention hors des locaux de la collectivité, les utilisateurs en assurent la garde et la responsabilité. Les utilisateurs ont dans cette hypothèse un niveau de surveillance et de confidentialité renforcées et doivent veiller à ce que des tiers non autorisés ne puissent accéder à ces moyens ni les utiliser.
En termes de sécurité et de confidentialité, les utilisateurs sont soumis aux mêmes obligations que les utilisateurs restant sur site. Ils devront suivre toutes les prescriptions complémentaires qui leur seront signifiées.

À l'extérieur de la collectivité, les utilisateurs devront privilégier une connexion par le biais des téléphones portables (via la fonction de partage de connexion) professionnels mis à disposition.

En cas de dysfonctionnement, de blocage, de perte ou de vol de l'équipement, les utilisateurs doivent en informer immédiatement l'Autorité territoriale. Ils doivent par ailleurs assister la collectivité, dans toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

10. DÉPART D'UN UTILISATEUR

Tout utilisateur, lors de la cessation de son activité au sein de la collectivité, perd son habilitation à utiliser les systèmes d'information internes.

Il doit :

- Restituer tous les matériels mis à sa disposition,
- Effacer de son poste de travail tous ses éventuels fichiers et données privées. Il ne peut effectuer une copie de son travail professionnel qu'après autorisation écrite de son supérieur hiérarchique dûment habilité. Les éventuels répertoires personnels ainsi que les données de messagerie des utilisateurs situés sur le serveur seront obligatoirement supprimés par l'administrateur informatique, en tout état de cause dans un délai maximum d'un mois après son départ.

11. MANQUEMENT À LA CHARTE

Le non-respect des règles édictées dans cette charte peut amener la collectivité à suspendre, voire supprimer, l'accès des contrevenants à ces outils de communication. En fonction de la gravité, des sanctions disciplinaires peuvent être prises selon la réglementation en vigueur dans la fonction publique territoriale et une procédure pénale peut être engagée.

Envoyé en préfecture le 22/11/2024
Reçu en préfecture le 22/11/2024
Publié le
ID : 087-218706505-20241120-2024_D_063-DE

12. OPPOSABILITÉ DE LA CHARTE

La présente charte est rendue opposable dès sa notification à l'ensemble des agents et des élus du conseil municipal.

Fait à FEYTIAT le,

Le Maire, GASTON CHASSAIN

L'utilisateur (Nom et signature) :

Vous déclarez avoir lu l'intégralité de la présente Charte, vous engagez à vous y conformer et reconnaissez que votre matériel, son contenu et l'utilisation du service Wifi sont de votre entière responsabilité.

Envoyé en préfecture le 22/11/2024
Reçu en préfecture le 22/11/2024
Publié le
ID : 087-218706505-20241120-2024_D_063-DE

ANNEXE : GLOSSAIRE

o Antivirus : logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants.

o Compte d'administrateur : compte permettant d'effectuer des modifications affectant les utilisateurs (modification des paramètres de sécurité, installer des logiciels…).

o Liens hypertextes : Un lien hypertexte est un élément placé dans le contenu d'une page Web ou d'un mail et qui permet, en cliquant dessus, d'accéder à un autre contenu sur une page interne (serveur) ou externe (page internet).

o Mise à jour : action qui consiste à mettre à niveau un outil ou un service informatique en téléchargeant un nouveau programme logiciel.

o Nomadisme : Le nomadisme numérique désigne toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité.

o Nom de domaine : identifiant de domaine internet. Un domaine est un ensemble d'ordinateurs reliés à Internet et possédant une caractéristique commune. A Feytiat , le nom de domaine est « ville-feytiat.fr »

o Pare-feu (firewall) : logiciel et/ou matériel permettant de protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet, protection d'un réseau d'entreprise, …) en filtrant les entrées et en contrôlant les sorties selon les règles définies par son utilisateur

o Phishing (hameçonnage) : méthode d'attaque qui consiste à imiter les couleurs d'une institution ou d'une société (banque, services des impôts) pour inciter le destinataire à fournir des informations personnelles.

o Système d'exploitation : logiciel qui, dans un appareil électronique, pilote les dispositifs matériels et reçoit des instructions de l'utilisateur ou d'autres logiciels

o Système d'information : c'est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un réseau d'ordinateurs o Télétravail : Le télétravail désigne toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon volontaire en utilisant les technologies de l'information et de la communication (article L. 1222-9 du code du travail). Le télétravail est donc une forme de nomadisme numérique.

o URL (Uniform Resource Locator) : Adresse d'un site ou d'une page hypertexte sur Internet.

o utilisateur : personne qui utilise un système informatique.

LES BASES LÉGALES :

L'utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 relative à la fonction publique territoriale. o Loi n° 78-17 du 6 janvier 1978 sur l'informatique, les fichiers, les libertés. Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

o Loi n° 78-753 du 17 juillet 1978 et l'ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration.

o 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.

o Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Elle est destinée à favoriser le développement des nouvelles technologies notamment par les collectivités.

Envoyé en préfecture le 22/11/2024
Reçu en préfecture le 22/11/2024
Publié le
ID : 087-218706505-20241120-2024_D_063-DE

LE DROIT DISCIPLINAIRE :

o Loi n° 83-634 du 13 juillet 1983 modifiée portant Droits et obligations des fonctionnaires modifiées.
o Loi n° 84-53 du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale.
o Décret n° 89-677 du 18 septembre 1989 modifié relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux.
o Décret n° 92-1194 du 4 novembre 1992 modifié fixant les dispositions communes applicables aux fonctionnaires stagiaires de la fonction publique territoriale
o Décret n° 88-145 du 15 février 1988 modifié pris pour l'application de l'article 138 de la loi du 28 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale et relatif aux agents non titulaires de la fonction publique territoriale.
o Décret n° 91-298 du 20 mars 1991 modifié portant dispositions statutaires applicables aux fonctionnaires territoriaux nommés dans des emplois permanents à temps non complet.