Envoyé en préfecture le 04/03/2025
Reçu en préfecture le 04/03/2025
Publié le 04/03/2025
ID : 044-214400301-20250226-D20250210-DE

Charte informatique
LA CHAPELLE DES MARAIS

La Charte d'utilisation des ressources informatiques, permet de définir les modalités d'utilisation des outils informatiques et de communication qu'utilisent quotidiennement les agents de la mairie de La Chapelle des Marais dans le cadre de leurs missions. Elle renforce la protection du réseau et veille à ce que les agents n'abusent pas des outils mis à leur disposition. En effet, les technologies informatiques et de communication apportent des améliorations de performance et de technicité offrant ainsi des moyens opérationnels pour réaliser son travail. Ces moyens opérationnels, pour qu'ils soient efficaces et efficients, doivent être maîtrisés, adaptés et contrôlés pour éviter qu'une mauvaise utilisation des outils technologiques puisse entrainer des conséquences préjudiciables pour les utilisateurs, voire pour la collectivité et les usagers.

Cette Charte n'a nullement pour finalité de contrôler le travail des agents ou de limiter l'utilisation quant aux outils informatiques et technologiques mis à leur disposition. Elle est avant tout, un guide de bonnes pratiques.

Préambule

La commune met à disposition de ses utilisateurs un système d'information (SI) et des moyens informatiques nécessaires à l'exécution de leurs missions et de leurs activités. Le SI comprend un réseau informatique, un réseau téléphonique et d'autres actifs régis par la charte. Les utilisateurs sont tenus d'utiliser les ressources informatiques mises à leur disposition par la mairie conformément aux règles définies dans la présente charte, le droit d'accès aux ressources numériques étant conditionné au respect de ladite charte.

Article 1 : Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs du système d'information, y compris les élus, les agents, les stagiaires, les employés de sociétés prestataires et les partenaires extérieurs. Les agents doivent faire accepter la présente charte à toute personne à laquelle ils permettraient l'accès au SI.

Article 2 : Périmètre du système d'information

Le système d'information est composé d'ordinateurs (fixes, légers, portables tablettes…), de téléphones (fixes, portables…), d'un réseau informatique (intranet, messagerie, internet, VPN…), de photocopieurs, de logiciels, d'applications bureautique, de logiciel métier, de bases de données informatisées et d'autres actifs régis par la charte. Tout matériel connecté au

Envoyé en préfecture le 04/03/2025
Reçu en préfecture le 04/03/2025
Publié le 04/03/2025
ID : 044-214400301-20250226-D20250210-DE

SI de la commune, y compris le matériel personnel des utilisateurs, est régi par la présente charte.

Les utilisateurs, devant réaliser des missions à domicile nécessitant l'utilisation des équipements informatiques de la commune, devront avoir l'autorisation du responsable de service. Ils devront prendre toutes les précautions pour assurer la sécurité des données « sorties » et de l'équipement matériel informatique mis à leur disposition. A ce titre, les utilisateurs devront justifier d'une assurance individuelle prenant en charge tout vol ou détérioration du matériel.

Article 3 : Règles générales d'utilisation

Le SI doit être utilisé à des fins professionnelles conformes aux objectifs de l'organisation, et dans le cadre des missions de l'agent sauf exception prévue par les présentes ou par la loi. Ils ne peuvent en aucun cas utiliser le SI de l'organisation pour se livrer à des activités concurrentes ou susceptibles de porter préjudice à l'organisation des services.

Article 4 : Sécurité informatique

La commune met en œuvre une série de moyens pour assurer la sécurité de son système d'information et des données traitées, en particulier des données personnelles. L'utilisateur est responsable des ressources informatiques qui lui sont confiées dans le cadre de ses missions et doit concourir à leur protection. Il doit s'assurer d'utiliser les ressources informatiques mises à sa disposition de manière raisonnable, conformément à ses missions. L'utilisateur s'engage à préserver la confidentialité des informations, en particulier des données personnelles, traitées sur le SI de l'organisation. Tout usage de clé USB, disque dur externe, n'appartenant pas à la commune devra avoir au préalable, été scanné par l'antivirus ou tout autre logiciel permettant la lutte contre les éléments malveillants. Le réseau wifi communal « MAIRIE » ne pourra être utilisé qu'à des fins professionnelles, un réseau wifi « PUBLIC » devra être utilisé pour tout autre appareil que ceux mis à disposition par la commune.

Article 5 : Modalités d'utilisation des ressources informatiques

L'utilisation des ressources du système d'information et l'usage des services Internet sont autorisés dans le cadre de l'activité professionnelle et présumés l'être à cette fin. Toute utilisation du système d'information est présumée professionnelle. L'utilisation de tels systèmes peut être le cas échéant pour des besoins personnels à la condition que cet usage présente un caractère limité en nombre et en durée de connexions, qu'il ne porte pas atteinte aux usages autorisés et ne nuit pas au bon fonctionnement du service.
L'accès aux réseaux et aux différents systèmes informatiques est strictement personnel et ne peut en aucun cas être cédé, même temporairement, à un tiers. Il peut être retiré à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle pour laquelle elle a été initialement concédée.

Envoyé en préfecture le 04/03/2025
Reçu en préfecture le 04/03/2025
Publié le 04/03/2025
ID : 044-214400301-20250226-D20250210-DE

Tout utilisateur ou utilisatrice est responsable de l'usage qu'il fait des ressources du système information auxquelles il a accès ainsi que du contenu de ce qu'il affiche, télécharge ou envoie. L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.
L'utilisateur a la charge, à son niveau, de contribuer à la sécurité générale du système d'information de la commune. Il doit notamment appliquer les recommandations de sécurité, assurer la protection de ses informations en utilisant les différents moyens de sécurité mis à sa disposition, en choisissant notamment des mots de passe sûrs et gardés secrets et être responsable du bon usage de ses droits. Le login et le mot de passe ont pour objectif de préserver la confidentialité des informations professionnelles.
En outre, l'utilisateur se doit de signaler toute anomalie qu'il peut constater au Responsable de la Sécurité des Systèmes d'Information (RSSI) de la commune, Franck Sauvage. En effet, l'employeur pourra demander à l'utilisateur de communiquer aux administrateurs ses mots de passe, s'il est absent et/ou lorsque cela s'avère nécessaire à la continuité du service public.
Il doit veiller à ne pas installer de logiciels, ni contourner ses restrictions d'utilisation.
Afin d'éviter tout usurpation d'identité, l'utilisateur doit veiller à ne pas laisser son matériel sans surveillance et sans se déconnecter (session, comptes…) en laissant des ressources ou services accessibles. Il ou elle doit également veiller à ne pas utiliser ou essayer d'utiliser des droits autres que les siens, de masquer sa véritable identité ou d'usurper celle d'autrui.

Article 6 : Accès à Internet et aux serveurs

L'accès à Internet est autorisé. Toutefois, pour des raisons de sécurité, l'accès à certains sites peut être limité.
Il appartient à l'utilisateur de procéder au stockage éventuel de ses fichiers à caractère privé dans un espace prévu explicitement à cet effet (espace exclusivement dénommé « privé » ou « personnel ») dont la responsabilité et la sauvegarde lui incombent. Cet espace est à localiser sur les disques durs du poste informatique et autres périphériques de l'utilisateur et en aucun cas sur les serveurs de fichiers (lecteurs réseaux nominatifs ou communs) ou sur un espace virtuel de stockage mis à sa disposition par la commune.
Afin d'assurer la continuité de service, l'utilisateur ou l'utilisatrice doit privilégier le dépôt de ses fichiers de travail sur des zones partagées par les membres de son service ou de son équipe.
En cas de départ, ou d'absence prolongée, l'utilisateur informe la commune des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition. En tout état de cause les données non situées dans un espace identifié comme privé, sont considérées comme appartenant à la commune qui pourra en disposer. Par ailleurs, de façon exceptionnelle, l'employeur peut être amené à accéder à la messagerie de l'utilisateur en son absence, lorsque cela est nécessaire à la continuité du service public.
L'utilisateur doit veiller à ne pas se connecter ou essayer de se connecter sur un serveur, interne ou externe, autrement que par les dispositions prévues par la Politique de Sécurité des Systèmes d'Information (PSSI) de la commune ou sans y être autorisé.

Envoyé en préfecture le 04/03/2025
Reçu en préfecture le 04/03/2025
Publié le 04/03/2025
ID : 044-214400301-20250226-D20250210-DE

Tout abonnement payant à un site Web ou à un service via internet doit faire l'objet d'une autorisation préalable de l'autorité territoriale.
Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède.
L'usage des ressources qui sont confiées à l'utilisateur ne doit pas être contraire à la réglementation en vigueur (ex : téléchargement illégal d'œuvres de l'esprit, visionnage illégal de programmes audiovisuels en « streaming »).
Enfin, il doit veiller à ne pas utiliser ces ressources pour proposer ou rendre accessibles aux tiers des données et informations confidentielles ou contraires à la législation en vigueur.
L'utilisateur doit faire preuve de la plus grande correction et discrétion à l'égard de ses interlocuteurs dans les échanges et notamment pour les courriers, forums de discussions, intranet, etc.
A cet égard, il doit notamment veiller à ne pas émettre d'opinions susceptibles de porter préjudice à la commune de La Chapelle des Marais, les élus et les agents communaux.
La commune de La Chapelle des Marais ne peut être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se conforme pas à ces règles.

Préalablement à la clôture de l'accès à la messagerie, l'utilisateur ou l'utilisatrice est invité(e) à faire le tri de ses messages préalablement à son départ, notamment à supprimer toutes données personnelles.

Article 7 : Email

Chaque agent qui en a l'utilité dispose d'une adresse email pour l'exercice de ses missions.
Tous les messages envoyés ou reçus sont présumés être envoyés à titre professionnel.
Les échanges électroniques avec des tiers ont la même valeur juridique que les échanges écrits. Un message électronique peut donc être une preuve ou un début de preuve, engageant l'utilisateur ou l'employeur au même titre qu'un courrier écrit.
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 pour pouvoir être protégés par le respect de la vie privée des agents et du secret des correspondances. Ils doivent enfin être classés dans un répertoire "PRIVE" dans la messagerie pour les messages reçus.
L'accès au service de messagerie a vocation à être fermé dès que l'utilisateur quitte les effectifs de la commune. Pour les agents, l'accès sera fermé le jour suivant leur départ.
Préalablement à la clôture de l'accès à la messagerie, l'utilisateur ou l'utilisatrice est invité(e) à faire le tri de ses messages préalablement à son départ, notamment à supprimer toutes données personnelles.

Envoyé en préfecture le 04/03/2025
Reçu en préfecture le 04/03/2025
Publié le 04/03/2025
ID : 044-214400301-20250226-D20250210-DE

Article 8 Responsabilités de l'employeur

L'employeur est à ce titre responsable des faits commis par ses agents au moyen de ses outils informatiques et de communication.
Dans le cadre de cette responsabilité, et lorsque l'employeur détient des présomptions sérieuses d'infraction aux règles de la charte, il peut être amené à contrôler la légalité de l'utilisation de ces outils par :

- une analyse du contenu des messages et fichiers professionnels
- une analyse des connexions internet par les fichiers de « trace » (dont la durée de conservation ne dépassera pas 6 mois)
- un blocage de l'accès à certains sites considérés comme dangereux ou interdits au regard de leur contenu présumé

Article 9 : Sanctions

Les manquements aux règles édictées par la présente charte peuvent engager la responsabilité de l'utilisateur et entraîner des sanctions à son encontre, telles que la limitation d'usage du SI et/ou des sanctions disciplinaires et/ou des poursuites judiciaires.

Article 10 : Information et entrée en vigueur

La présente charte a été validée par la Commission des Finances - RH et Administration Générale du 09 septembre 2024, ainsi que par le Conseil Municipal du 26 février 2025, et entre en vigueur à la date du 27 février 2025.

La présente charte est modifiable en fonction des évolutions de logiciels ou de pratiques ou propositions d'utilisateurs

Envoyé en préfecture le 04/03/2025
Reçu en préfecture le 04/03/2025
Publié le 04/03/2025
ID : 044-214400301-20250226-D20250210-DE

Annexe 1 Fiche réflexe à destination des agents en cas de cyber attaque

FICHE REFLEXE
INCIDENT CYBER

Les consignes suivantes doivent être appliquées

immédiatement après le déclenchement de l'antivirus ou en cas de fonctionnement anormal de l'ordinateur.

1. • DÉCONNECTER LA MACHINE DU RESEAU
2. • NE PAS ÉTEINDRE L'ORDINATEUR
3. • **RENDRE COMPTE IMMÉDIATEMENT A VOTRE RESPONSABLE INFORMATIQUE**
4. • IDENTIFIER CLAIREMENT LA MACHINE COMME INFECTÉE **PAR L'APPOSITION D'UN VISUEL (étiquette,post-it etc..).**
5. • INTERDIRE L'ACCÈS A CETTE MACHINE.
6. • RASSEMBLER TOUS LES SUPPORTS INFORMATIQUES (Clés USB, disque externe, etc...) UTILISÉS SUR L'ORDINATEUR ET LES CONSERVER.

☎ Prévenir le service informatique / Responsable informatique

Déconnexion du réseau :

Identifier la prise réseau (exemple ci-contre) allant de l'ordinateur à la prise murale et la déconnecter de l'ordinateur en appuyant sur la petite languette située sur la prise.

Envoyé en préfecture le 04/03/2025
Reçu en préfecture le 04/03/2025
Publié le 04/03/2025
ID : 044-214400301-20250226-D20250210-DE

FORMULAIRE A REMPLIR

CHARTE INFORMATIQUE DE LA COMMUNE DE LA CHAPELLE DES MARAIS

Nom et Prénom :

.....

Poste/ Qualité :

.....

Service :

.....

Adresse courriel :

.....

Déclare avoir pris connaissance de la charte informatique de la commune de La Chapelle des Marais et accepte de s'y conformer

A La chapelle des Marais, le