CHARTE DE BON USAGE DES MOYENS INFORMATIQUES ET DE TÉLÉCOMMUNICATIONS

Table des matières

1. Objet du document 3
2. Champ d'application 3
3. Cadre réglementaire 4
4. Critères fondamentaux de la sécurité 4
   4.1. Principes 4
   4.2. Une mission sécurité 5
   4.3. Un enjeu technique et organisationnel 5
   4.4. Une gestion des risques 5
5. Règles de sécurité 5
   5.1. Confidentialité de l'information et obligation de discrétion 7
   5.2. Protection de l'information 7
   5.3. Usage des ressources informatiques 8
   5.4. Usage des outils de communication 8
      5.4.1. Usage du téléphone 8
      5.4.2. Usage d'Internet 9
      5.4.3. Usage de la messagerie 10
      5.4.4. Envoi de messages électroniques 10
      5.4.5. Utilisation des badges électroniques 11
      5.4.6. Signature électronique et certificats 11
   5.5. Usage des login et des mots de passe 11
   5.6. Utilisation des médias sociaux 12
   5.7. Photographies-droit à l'image 12
   5.8. Image de marque de la commune de Saint-Pierre-Lès-Elbeuf et du CCAS 12
   5.9. Téléassistance informatique 12
   5.10. Absence de l'agent 13
   5.11. Départ de l'agent 13
6. Protection des données personnelles 13
7. Surveillance du système d'information 14
   7.1. Contrôle 14
   7.2. Traçabilité 14
   7.3. Alertes 15
8. Responsabilités et sanctions 15
9. Opposabilité 16
10. Entrée en vigueur 16

1. OBJET DU DOCUMENT

La présente charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet de la commune et du CCAS de Saint-Pierre-lès-Elbeuf.
Elle rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information. Elle pose des règles permettant d'assurer la sécurité et la performance du système d'information de la commune et du CCAS, de préserver la confidentialité des données dans le respect de la réglementation en vigueur et des droits et libertés reconnus aux utilisateurs, conformément à la politique de sécurité du système d'information définie par la commune et le CCAS.

Cette charte est susceptible d'être modifiée en fonction des évolutions technologiques et réglementaires.

Chaque utilisateur s'engage à la respecter.

2. CHAMP D'APPLICATION

La présente charte concerne les ressources informatiques, les services Internet et téléphoniques de la commune et du CCAS de Saint-Pierre-lès-Elbeuf, ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électronique interne ou externe.

Il s'agit principalement des ressources suivantes :

- Ordinateurs de bureau
- Ordinateurs portables
- Imprimantes et photocopieurs multifonction
- Téléphones portables, tablettes, téléphonie fixe sous IP.

Cette liste est susceptible d'évoluer en fonction des usages.

Cette charte s'applique à l'ensemble du personnel utilisant les moyens informatiques de la commune et du CCAS tous statuts confondus (titulaires, stagiaires, contractuels, saisonniers, occasionnels….) mais aussi aux élus, prestataires, partenaires et tout autre utilisateur.
Cette liste non nominative évoluera en fonction des usages. Dans la présente charte, sont désignés sous les termes suivants :

- **Ressources informatiques** : les moyens informatiques, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'entité ;
- **Outils de communication** : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses (web, messagerie, etc.) ;
- **Utilisateurs** : les personnes ayant accès ou utilisant les ressources informatiques et les services Internet de la commune et du CCAS.

3. CADRE REGLEMENTAIRE

Le cadre réglementaire de la sécurité de l'information est complexe. Il porte sur les grands thèmes suivants :

- le traitement de données à caractère personnel et le respect de la vie privée ;
- l'hébergement de données ;
- le secret professionnel ;
- le secret des correspondances ;
- la lutte contre la cybercriminalité ;
- la protection des logiciels et des bases de données et le droit d'auteur.

La présente charte tient compte de la réglementation sur la sécurité de l'information en vigueur et des droits et libertés reconnus aux utilisateurs.

Fondements législatifs et réglementaires applicables :
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- Code général de la Fonction publique ;
- Règlement UE 2016/679 dit Règlement général sur la protection des données (RGPD) ;
- Loi n°2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires ;
- Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles ;
- Le Code du travail, dans son application par exception à la fonction publique territoriale.

4. CRITERES FONDAMENTAUX DE LA SECURITE

4.1. Principes

La commune et le CCAS de Saint-Pierre-lès-Elbeuf hébergent des données et des informations administratives sur ses administrés, agents, fournisseurs, …
L'information se présente sous de multiples formes : stockée sous forme numérique sur des supports informatiques, imprimée ou écrite sur papier, transmise par des réseaux informatiques privés ou Internet, par la poste, oralement et/ou par téléphone,...

La sécurité de l'information est caractérisée comme étant la préservation de :

- **sa disponibilité** : l'information doit être accessible à l'utilisateur, quand celui-ci en a besoin ;
- **son intégrité** : l'information doit être exacte, exhaustive et conservée intacte pendant sa durée de vie ;
- **sa confidentialité** : l'information ne doit être accessible qu'aux personnes autorisées à y accéder ;
- **sa traçabilité** : les systèmes doivent comporter des moyens de preuve sur les accès et opérations effectuées sur l'information.

4.2. Une mission sécurité

La Direction et le Responsable des systèmes d'information, fournissent un système d'information qui s'appuie sur une infrastructure informatique. Elle doit assurer la mise en sécurité de l'ensemble c'est-à-dire protéger ces ressources contre des pannes, des erreurs ou des malveillances. Elle doit aussi protéger les intérêts économiques de la structure en s'assurant que ces moyens sont bien au service de la production de la commune et du CCAS de Saint Pierre-lès-Elbeuf. Elle doit donc définir et empêcher les abus.

4.3. Un enjeu technique et organisationnel

Les enjeux majeurs de la sécurité sont la qualité et la continuité des services, le respect du cadre juridique sur l'usage des données personnelles.

Pour cela, la Direction et le Responsable des systèmes d'information, déploient un ensemble de dispositifs techniques mais aussi organisationnels. En effet, au-delà des outils, la bonne utilisation des moyens informatiques est essentielle pour garantir un bon niveau de sécurité. La sécurité peut être assimilée à une chaîne dont la solidité dépend du maillon le plus faible. Certains comportements humains, par ignorance des risques, peuvent fragiliser le système d'information.

4.4. Une gestion des risques

La sécurité repose sur une gestion des risques avec des analyses des risques potentiels, des suivis d'incidents, des dispositifs d'alertes. La communication vers les utilisateurs est un volet important de cette gestion. La présente charte s'inscrit dans ce plan de communication.

5. REGLES DE SECURITE

L'accès au système d'information de la commune et du CCAS de Saint-Pierre-lès-Elbeuf est soumis à autorisation. Une demande préalable est ainsi requise pour l'attribution d'un accès aux ressources informatiques, aux services Internet et de télécommunication ; cette demande est exprimée par le supérieur hiérarchique de l'utilisateur, qui précise les accès nécessaires à son collaborateur et la transmet par le biais d'une demande inter-service (voie électronique) au Responsable du pôle informatique et ressources numériques.

Le pôle informatique et ressources numériques attribue à chaque utilisateur (après avoir signé cette présente charte), si besoin, des droits d'accès aux ressources informatiques. Ce droit d'accès est strictement personnel et concédé à l'utilisateur pour des activités exclusivement professionnelles. Il ne peut être cédé, même temporairement à un tiers. Tout droit prend fin lors de la cession, même provisoire, de l'activité professionnelle de l'utilisateur, ou en cas de non- respect des dispositions de la présente charte par l'utilisateur.

L’obtention d’un droit d’accès au système d’information entraîne pour l’utilisateur les droits et les responsabilités précisées dans les paragraphes ci-dessous.

L'utilisateur ne doit pas utiliser ou essayer d'utiliser des comptes d'accès aux réseaux autres que le sien ou masquer sa véritable identité. Il est en particulier interdit d'utiliser une session ouverte par quelqu'un d'autre.
L'utilisateur s'engage à :

- ne pas mettre à la disposition de personnes non autorisées un accès au système
- éteindre son poste par arrêt logiciel et non par l'interrupteur pour terminer ses sessions
- ne jamais quitter le poste de travail en laissant une session ouverte en cours et toujours verrouiller la session ouverte en cours
- ne pas laisser à disposition des supports informatiques (CDrom, clés USB ...) contenant des données confidentielles, dans un bureau ouvert
- éteindre son poste de travail chaque soir lors de son départ des locaux de la Ville
- protéger les données dont l'utilisateur est responsable, en utilisant les moyens de sauvegarde mis à sa disposition
- respecter la confidentialité des informations relatives à la Ville
- ne pas extraire et consulter les données confidentielles de la Ville dans les lieux publics
- ne pas perturber le bon fonctionnement du système d'information en faisant une utilisation rationnelle des ressources partagées (impressions de gros documents, utilisation intensive du réseau…)
- ne pas connecter sur le réseau de la Ville un ordinateur externe sans un contrôle préalable du poste par le pôle informatique et ressources numériques et sans vérification des anti-virus à jour
- ne pas installer ni faciliter l'installation par un tiers, de logiciels ou de matériels informatiques n'appartenant pas à la Ville et sans autorisation du pôle informatique et ressources numériques (ordinateur portable, smartphone, tablettes)
- signaler sans délai au service informatique tout incident de sécurité ou dysfonctionnement du système d'information qu'il serait amené à constater ou à subir (virus, destruction, vol, anomalie concernant les droits d'accès).

Il est en outre demandé à tout utilisateur, en particulier concernant l'utilisation des imprimantes connectées au réseau informatique de la Ville :

- de privilégier les impressions en mode recto/verso
- de privilégier de façon quotidienne les impressions en noir et blanc et, pour celles ou ceux y ayant accès, limiter les impressions couleur aux seuls documents nécessitant ce traitement
- ne pas oublier de récupérer sur les imprimantes ou photocopieurs, les documents sensibles que l'on envoie, imprime ou photocopie
- de conserver les documents et archives confidentiels dans un endroit sécurisé
- de ne pas laisser sur leur bureau des documents confidentiels
- de privilégier les broyeurs de documents pour la destruction des impressions «sensibles», « confidentiels » ou contenant des données nominatives.

5.1. Confidentialité de l'information et obligation de discrétion

Les personnels de la commune et du CCAS de Saint-Pierre-lès-Elbeuf sont soumis au secret professionnel. Les personnels se doivent de faire preuve d'une discrétion absolue dans l'exercice de leur mission. Un comportement exemplaire est exigé dans toute communication, orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés. Il est ainsi interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courrier électroniques dont l'utilisateur n'est ni directement destinataire, ni en copie.

L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ ou confidentielles couvertes par le secret professionnel.

5.2. Protection de l'information

Les postes de travail permettent l'accès aux applications du système d'information. Ils permettent également d'élaborer des documents bureautiques. Il est important d'éviter de stocker des données et des documents sur ces postes (disques durs locaux). Les documents bureautiques produits doivent être stockés de préférence sur des serveurs de fichiers (SERGED). Ces espaces sont à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit.

Les bases de données associées aux applications métiers, quand elles ne sont pas gérées de manière externalisée (hébergement externalisé), sont implantées sur des serveurs hébergés dans une salle protégée des locaux de la mairie.
Le cas échéant, ceux qui utilisent un matériel portable (exemples : poste, tablette, smart phone,…) ne doivent pas le mettre en évidence pendant un déplacement, ni exposer son contenu à la vue d'un voisin de train … ; le matériel doit être rangé en lieu sûr. De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (exemples : CD, clé USB, disque dur, …).
L'usage de tous supports de stockage amovibles personnels (clé USB, disque dur externe, CD, DVD...) est strictement interdite. Seules ceux dédiés à la commune sont autorisés.
Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.
Les médias de stockage amovibles (exemples : clefs USB, CD-ROM, disques durs …) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus) ou risques de perte de données. L'utilisation de ces outils de stockage amovibles est vivement déconseillée.
L'utilisateur ne doit pas transmettre de fichiers sensibles à une personne qui en ferait la demande et qu'il ne connaîtrait pas, même s'il s'agit d'une adresse électronique interne à la commune et au CCAS.

5.3. Usage des ressources informatiques

Tout utilisateur s'engage :

1. à ne pas installer de nouveaux matériels, logiciels mêmes gratuits, à ne pas modifier les configurations systèmes ou toutes autres actions tendant à modifier le fonctionnement des matériels et logiciels sauf autorisation expresse du pôle informatique et ressources numériques
2. à ne déconnecter du réseau aucun matériel informatique ou téléphonique sauf autorisation expresse du pôle informatique et ressources numériques
3. à ne pas accéder ou essayer d'accéder à des informations auxquelles il n'a pas accès
4. à ne pas modifier ou détruire des informations communes (fichiers de groupe, données de bases de données) au-delà de la limite de son champ d'activité
5. à ne pas procéder à des téléchargements de fichiers n'entrant pas dans son champ d'activité (musique, vidéo, image..) et couverts par les lois sur la propriété intellectuelle
6. à prendre soin du matériel mis à sa disposition et à signaler au pôle informatique et ressources numériques tout dysfonctionnement.

5.4. Usage des outils de communication

Les outils de communication tels que le téléphone, Internet ou la messagerie sont destinés à un usage exclusivement professionnel. L'usage à titre personnel, dans le cadre des nécessités de la vie privée, est toléré à condition qu'il ne nuise pas à la qualité et au fonctionnement du service. Cette utilisation doit être occasionnelle, non lucrative et raisonnable et qu'elle ne puisse pas porter atteinte à l'image de marque de la collectivité. Il ne doit en aucun cas être porté à la vue de personnes extérieures.

5.4.1. Usage du téléphone

Le téléphone est un des moyens potentiels d'échanges de données qui présentent des risques puisque l'identité de l'interlocuteur qui répond au téléphone n'est pas garantie.

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un téléphone fixe et/ou mobile, d'un smartphone, d'une tablette.

Concernant l'utilisation des terminaux mobiles en connexion pour accès à des sites Internet ou à la messagerie électronique, les règles édictées dans la présente charte s'appliquent identiquement.

L'utilisateur ne doit communiquer aucune information sensible par téléphone, notamment des informations nominatives, ainsi que des informations ayant trait au fonctionnement interne de la commune et du CCAS de Saint-Pierre-Lès-Elbeuf. Si un doute subsiste, le numéro de téléphone de l'interlocuteur indiqué doit être vérifié.

L'utilisateur s'engage en outre à :

- prévenir la Direction sans délai en cas de perte, vol ou faille de sécurité
- mettre en œuvre tous les moyens de sécurité prévus par les fonctionnalités du smartphone et qui sont demandées et notamment le code d'accès
- être vigilants vis à vis des données contenues dans le smartphone

La vigilance de l'utilisateur est attirée sur le fait que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel.
L'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites raisonnables en termes tant de temps passé que de quantité d'appels.

Le pôle informatique et ressources numériques, à travers un logiciel de gestion de flotte mobile pourra limiter et contraindre l'utilisation du téléphone.

5.4.2. Usage d'Internet

L'accès à Internet est un outil de travail et a pour objectif d'aider les personnels à trouver des informations nécessaires à leur mission usuelle, ou dans le cadre de projets spécifiques.

Il est rappelé aux utilisateurs que, lorsqu'ils « naviguent » sur Internet, les informations de navigation peuvent être enregistrées. Il conviendra donc d'être particulièrement vigilant lors de l'utilisation de Internet et à ne pas mettre en danger l'image ou les intérêts de la commune et du CCAS de Saint-Pierre-Lès-Elbeuf.

Par ailleurs, les données concernant l'utilisateur (exemples : sites consultés, messages échangés, données fournies à travers un formulaire, données collectées à l'insu de l'utilisateur,…) peuvent être enregistrées par des tiers, analysées et utilisées à des fins notamment commerciales. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur Internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle.

Il est interdit de se connecter ou de tenter de se connecter à Internet par des moyens autres que ceux fournis par la commune et le CCAS. Il est interdit de participer à des forums, blogs et groupes de discussion à des fins non professionnelles, et de se connecter sur des sites à caractère injurieux, violent, raciste, discriminatoire, sexiste, pornographique, diffamatoire ou manifestement contraire à l'ordre public.

En outre, l'utilisateur s'engage expressément :

1. à respecter les lois et règlements en vigueur sur le territoire français
2. à ne pas stocker ou diffuser de messages dont le contenu serait contraire au respect de la dignité humaine, de l'ordre public ou constituant une incitation à la pédophilie, au racisme au terrorisme, à la xénophobie, à des trafics divers et variés ou à la promotion de mouvements sectaires
3. à ne pas fournir un soutien au piratage ou à une atteinte à la sécurité nationale.

5.4.3. Usage de la messagerie

La messagerie permet de faciliter les échanges entre les professionnels de la collectivité, les organismes, les fournisseurs,…

Les utilisateurs doivent garder à l'esprit que leurs messages électroniques peuvent être stockés, réutilisés, exploités à des fins auxquelles ils n'auraient pas pensé en les rédigeant, constituer une preuve ou un commencement de preuve par écrit ou valoir offre ou acceptation de manière à former un contrat entre la commune ou le CCAS et son interlocuteur, même en l'absence de contrat signé de façon manuscrite.

Toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent donc à la messagerie. L'envoi de messages électroniques doit respecter les mêmes procédures de contrôle, de validation, d'autorisation que les courriers.
Il est souhaitable de mettre systématiquement en copie des messages importants son responsable et le responsable du destinataire, et il est obligatoire de transmettre pour validation à un responsable tout message qui aurait valeur contractuelle ou d'engagement.
Par ailleurs, tout message important doit être conservé à des fins d'archivage.
Un usage privé de la messagerie est toléré s'il reste exceptionnel.

Il est strictement interdit d'utiliser la messagerie pour des messages d'ordre commercial ou publicitaire, du prosélytisme, du harcèlement, des messages insultants ou de dénigrement, des textes ou des images ou vidéos provocants et/ou illicites, ou pour propager des opinions personnelles, qui pourraient engager la responsabilité de la commune et du CCAS de Saint-Pierre-Lès-Elbeuf ou de porter atteinte à son image. Les utilisateurs sont tenus par leurs clauses de confidentialité et de loyauté contractuelles dans le contenu des informations qu'ils transmettent par email.

Il est strictement interdit d'ouvrir ou de lire des messages électroniques d'un autre utilisateur, sauf si ce dernier a donné son autorisation explicite.

L'hameçonnage (phishing), point d'entrée de la majorité des cyberattaques, est devenu un véritable fléau pour les organisations de toute taille. Dans ce cadre, les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un filtrage anti-spam. Toutefois, ce dispositif n'est pas infaillible. Les utilisateurs sont donc invités à apporter la plus grande vigilance et à informer le pôle informatique et ressources numériques au moindre message douteux.

5.4.4. Envoi de messages électroniques

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel.

La forme des messages professionnels doit respecter les règles de courtoisie habituelles.

5.4.5. Utilisation des badges électroniques

Certains utilisateurs disposent de badges électroniques nominatifs et non cessibles permettant d'accéder aux locaux de la collectivité. Ceux-ci sont connectés aux logiciels de contrôle d'accès des bâtiments concernés qui enregistrent les horaires d'entrée et de sortie.

5.4.6. Signature électronique et certificats

Certains utilisateurs, dans le cadre de leurs fonctions, sont amenés à utiliser les 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.
L'utilisateur doit ainsi veiller à garder confidentiel le code saisi (clé privée) lors de la signature de son certificat.

5.5. Usage des login et des mots de passe

Chaque utilisateur dispose de compte nominatif lui permettant d'accéder aux applications et aux systèmes informatiques de la commune et du CCAS. Ce compte est personnel mais peut toutefois être un compte de service. Il est strictement interdit d'usurper une identité en utilisant ou en tentant d'utiliser le compte d'un autre utilisateur ou en agissant de façon anonyme dans le système d'information.

Pour utiliser ce compte nominatif, l'utilisateur dispose d'un login et d'un mot de passe.

Le mot de passe choisi doit être de préférence simple à mémoriser, mais surtout complexe à deviner : huit caractères minimum comprenant si possible au moins une majuscule, une minuscule, un chiffre et un symbole ($, % , ?, @…).
Pour des raisons de sécurité, le pôle informatique et ressources numériques peut imposer un changement de mot de passe.
Le mot de passe est strictement confidentiel. Il ne doit pas être communiqué à qui que ce soit.

Chaque utilisateur est responsable de son compte et de son mot de passe, et de l'usage qui en est fait. Il ne doit ainsi pas mettre à la disposition de tiers non autorisés un accès aux systèmes et aux réseaux de la commune et du CCAS dont il a l'usage. Pour cela, il convient de fermer ou verrouiller sa session lorsqu'on quitte son poste.
Il est interdit de contourner ou de tenter de contourner les restrictions d'accès aux logiciels. L'utilisateur s'engage enfin à signaler toute tentative de violation de son compte personnel.
L'emploi de mots de passe commun à plusieurs personnes est interdit. Néanmoins cette disposition ne s'applique que lorsque les comptes de messagerie sont liés à une fonction bien précise (messagerie de service).
Seules les personnes du pôle informatique et ressources numériques peuvent exceptionnellement être amenées à utiliser un mot de passe d'un utilisateur, avec son accord, pour résoudre un problème que ce dernier leur aura signalé.

5.6. Utilisation des médias sociaux

Les plateformes sociales sont des véritables espaces publics, visibles et consultables par tous. Tout le monde peut propager vos idées en republiant un contenu écrit, vidéo ou audio instantanément. Par ailleurs, l'agent est impliqué personnellement sur tout ce que qu'il publie ou retransmet (partage, ''like'', retweet, commentaire, etc..).

La facilité d'accès, l'illusion d'anonymat sur les réseaux sociaux, ne doivent pas faire oublier aux agents l'exercice de leurs obligations, qui continuent à s'appliquer même en dehors du cadre professionnel. Aussi bien sur les réseaux gérés par la commune et le CCAS que sur ses réseaux personnels, chaque agent demeure soumis aux obligations de réserve, de discrétion et de secret professionnel. A ce titre, il leur est demandé notamment de faire preuve de mesure dans leurs propos afin de ne pas porter atteinte à l'image ou à la considération de la collectivité et du CCAS.

Les informations postées par les utilisateurs sont indexées par les moteurs de recherche. Elles laissent des traces durables qui peuvent suivre un utilisateur tout au long de sa vie. Il est donc nécessaire de s'exprimer en toute connaissance des sujets traités. L'agent ne doit pas engager la collectivité sur ses réseaux sociaux personnels.
L'usage des réseaux sociaux durant le temps de travail doit rester limité à un usage professionnel.

Il est interdit aux agents non habilités de commenter toute publication en lien avec les actions de la collectivité sur l'ensemble des réseaux sociaux.

5.7. Photographies-droit à l'image

L'image d'une personne ne peut être utilisée sans son consentement. Les photos prises dans le cadre des activités de la collectivité ou dans ses locaux ne peuvent pas être utilisées à des fins personnelles et sont interdites à la diffusion externe sans le consentement de la direction. Cette recommandation s'applique aux enregistrements sonores et vidéo.

5.8. Image de marque de la commune Saint-Pierre-Lès-Elbeuf et du CCAS

Les utilisateurs de moyens informatiques ne doivent pas nuire à l'image de marque de la collectivité en utilisant des moyens, que ce soit en interne ou en externe, à travers des communications d'informations à l'extérieur de la commune et du CCAS ou du fait de leurs accès à Internet.

5.9. Téléassistance informatique

Le pôle informatique et ressources numériques de la commune et du CCAS de Saint-Pierre-Lès-Elbeuf dispose d'outils de prise en main à distance pour dépanner et/ou accompagner les utilisateurs dans leur quotidien informatique.
Ces actions se feront toujours avec l'accord de l'utilisateur final ; qui sera averti par une demande de confirmation affichée à l'écran pour valider la prise en main ou par sa communication des identifiants et mots de passe de l'outil de dépannage.

5.10. Absence de l'agent

Dans le cas où un agent serait absent, la continuité de service doit obligatoirement être assurée. Ainsi, l'agent doit veiller à ce que son service puisse continuer à accéder aux documents, logiciels et dossiers indispensables à l'activité (transmission des documents et dossiers aux collègues, ou mis à disposition dans un dossier partagé, création de compte pour accéder aux applications, à l'exclusion de toute communication des mots de passe personnels).
Dans le cas d'une absence imprévue (maladie, accident, …) ne pouvant être compensée par une activité de télétravail, le supérieur hiérarchique pourra demander au pôle informatique et ressources numériques l'accès à l'espace de travail de l'agent.

5.11. Départ de l'agent

En cas de départ définitif ou de mutation d'un agent, son successeur récupérera les documents de travail de son prédécesseur et ses accès aux ressources informatiques.
Concernant la messagerie, le successeur pourra récupérer l'intégralité des emails de son prédécesseur à l'exception des documents et emails d'ordre privé.

6. PROTECTION DES DONNEES PERSONNELLES

Le règlement général sur la protection des données ou « RGPD », accorde aux personnes physiques certains droits relatifs à leurs données personnelles qui sont :

- droit d'accès : le droit d'être informé et de demander l'accès aux données personnelles que la collectivité traite,
- droit de rectification : le droit de demander de modifier ou de mettre à jour les données personnelles lorsqu'elles sont inexactes ou incomplètes,
- droit d'effacement : le droit de demander de supprimer définitivement les données personnelles,
- droit de restriction : le droit de demander d'arrêter temporairement ou définitivement le traitement de tout ou partie des données personnelles,
- droit d'opposition : droit de refuser à tout moment le traitement des données personnelles pour des raisons personnelles, ou pour des fins de marketing direct,
- droit à la portabilité des données : le droit de demander une copie de vos données personnelles au format électronique et le droit de transmettre ces données personnelles pour une utilisation par un service tiers.

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a créé un dispositif juridique pour encadrer la mise en œuvre des « traitements automatisés de données à caractère personnel ».
Les données à caractère personnel sont des informations qui permettent directement ou indirectement l'identification des personnes physiques auxquelles elles s'appliquent.
L'utilisateur doit donc avant toute création de fichier comprenant ce type d'information, y compris lorsqu'elle résulte d'interconnexions de fichiers existants, accomplir les formalités prévues par la loi et qui s'exercent auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL). Ces formalités doivent s'effectuer selon la procédure définie. Par ailleurs, la loi ouvre aux personnes un droit d'accès et de rectification sur les données les concernant.

7. SURVEILLANCE DU SYSTEME D'INFORMATION

Cette section décrit le dispositif de surveillance du système d'information mis en œuvre par la commune et le CCAS, et notamment les modalités de contrôle de l'usage du système d'information par les utilisateurs et la gestion des traces. Il convient ainsi d'adapter cette section aux modalités de surveillance du système d'information déjà mises en place au sein de la commune et le CCAS de Saint-Pierre-Lès-Elbeuf.

7.1. Contrôle

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment de la loi Informatique et Libertés.

Mention légale :

La maire de la commune de Saint-Pierre-Lès-Elbeuf sis à place François Mitterrand 76320 Saint-Pierre-Lès-Elbeuf a désigné l'ADICO sis à Beauvais (60000), 5 rue Jean Monnet en qualité de Délégué à la Protection des Données (DPO). Les données recueillies via le système de journalisation des accès sont destinées à la réalisation du traitement : traçabilité des activités de chaque utilisateur sur les postes informatiques. Ce traitement est basé sur l'intérêt légitime.
Les données ne sont destinées qu'à la Mairie de Saint-Pierre-Lès-Elbeuf et ne sont transmises à aucun tiers.
Conformément aux articles 15 à 22 du règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016, chaque utilisateur dispose d'un droit d'accès, de rectification, d'effacement, de limitation, d'opposition et de portabilité des données le concernant.
Pour exercer ces droits, nous invitons l'utilisateur à contacter la Mairie de Saint-Pierre-Lès-Elbeuf sis à place François Mitterrand 76320 Saint-Pierre-Lès-Elbeuf. Si ce dernier estime, après nous avoir contactés, que ses droits ne sont pas respectés, il peut adresser une réclamation en ligne ou par voie postale à la CNIL.

7.2. Traçabilité

Le Responsable des systèmes d'information, assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition pour des raisons d'exigence réglementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

Par conséquent, les applications de la collectivité, ainsi que les réseaux, messagerie et accès Internet intègrent des dispositifs de traçabilité permettant d'enregistrer :

- l'identifiant de l'utilisateur ayant déclenché l'opération ;
- l'heure de la connexion ;
- le système auquel il est accédé ;
- le type d'opération réalisée.

Le personnel informatique respecte la confidentialité des données et des traces auxquelles ils sont amenés à accéder dans l'exercice de leur fonction, mais peuvent être amenés à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

7.3. Alertes

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la sécurité ou manquement substantiel à cette charte doit être signalé au Délégué à la Protection des Données Personnelles.

La sécurité de l'information met en jeu des moyens techniques, organisationnels et humains. Chaque utilisateur de l'information se doit d'avoir une attitude vigilante et responsable afin que les usagers bénéficient d'une prise en charge sécurisée et que leur vie privée ainsi que celle des personnels soient respectées

8. RESPONSABILITES ET SANCTIONS

Ce document est fondé sur le respect traditionnel des droits et des devoirs des fonctionnaires dans le cadre de leur mission de service public afin d'éviter que l'utilisation des moyens informatiques ne se retourne contre l'agent ou contre l'administration elle-même.

Les règles définies dans la présente charte ont été fixées dans le respect des dispositions législatives et réglementaires applicables.

La collectivité ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé aux règles d'accès et d'usage des ressources informatiques et des services Internet décrites dans la charte.
Il est rappelé que la présente charte est un document à portée juridique, et donc contraignante pour les utilisateurs.

En effet, le manquement aux règles et mesures de sécurité décrites dans 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.
La ville se réserve également le droit d'engager ou de faire engager des poursuites pénales et/ou civiles, indépendamment des sanctions disciplinaires mises en œuvre, notamment mais pas limitativement en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret des correspondances.

La loi et les textes réglementaires précisent les droits et devoirs des utilisateurs d'informatique (article 226 - 16 à 226 - 24 du code pénal).
Le non-respect de la présente charte entraîne l'application de sanctions disciplinaires, civiles et/ou pénales en relation avec la nature et la gravité des faits constatés.

9. OPPOSABILITE

La présente charte est rendue opposable dès sa notification à chaque utilisateur valant acceptation entière de ses termes.
L'accès aux ressources informatiques ne pourra se faire qu'après acceptation des modalités précisées dans la charte. Cette acceptation est matérialisée par la remise à l'agent d'un exemplaire de cette charte et la signature d'un récépissé. Le pôle informatique et ressources numériques met en place toutes les mesures techniques nécessaires à son application et au contrôle de son exécution.

10. ENTREE EN VIGUEUR

Cette présente charte est effective après avis du Comité Social Territorial du 31 mars 2023 et du Conseil Municipal du 11 mai 2023.