AUCAMVILLE

AUCAMVILLE
Centre Communal d'Action Sociale

CHARTE DE BON USAGE

DES MOYENS

INFORMATIQUES ET DE

TELECOMMUNICATIONS

Table des matières

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 d'Aucamville.
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 a été validée par la Direction générale de la commune d'Aucamville et présentée au Comité technique du 29 mars 2021. Elle est susceptible d'être modifiée en fonction des évolutions technologiques et règlementaires.

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 d'Aucamville, 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, tablettes ;
- Terminaux portables ;
- Imprimantes simples ou multifonctions ;
- Téléphones portables, téléphonie fixe sous IP.

Cette liste est non nominative et évoluera 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 d'accès et d'usage du système d'information tient compte de la réglementation sur la sécurité de l'information en vigueur et des droits et libertés reconnus aux utilisateurs.

4. CRITERES FONDAMENTAUX DE LA SECURITE

4.1. Principes

La commune et le CCAS d'Aucamville 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, fournit 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 d'Aucamville. 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, déploie 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 d'accès et d'usage du système d'information s'inscrit dans ce plan de communication.

5. REGLES DE SECURITE

L'accès au système d'information de la commune et du CCAS d'Aucamville est soumis à autorisation. Une demande préalable écrite est ainsi requise pour l'attribution d'un accès aux ressources informatiques, aux services Internet et de télécommunication ; la demande exprimée par l'utilisateur est au préalable validée par son responsable, qui précise les accès nécessaires à son collaborateur et la transmet par écrit au Responsable des systèmes d'information.

Le service informatique attribue alors au demandeur son droit d'accès après s'être assuré que le demandeur a pris connaissance de la présente charte et signé le récépissé. 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 ;
- ne pas répondre aux messages en masse ou en chaîne des messageries ;
- 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 service informatique 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 service informatique (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 limiter les impressions couleur aux seuls documents nécessitant ce traitement ;
- ne pas oublier de récupérer, sur les fax, 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 d'Aucamville sont soumis au secret professionnel. Cette obligation revêt une importance toute particulière lorsqu'il s'agit de conformité au RGPD. 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'accès aux données à caractère personnel par des professionnels habilités se fait par login et mot de passe.

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 de ne stocker aucune donnée ni aucun document sur ces postes (disques durs locaux). Les bases de données associées aux applications métiers sont implantées sur des serveurs hébergés dans une salle protégée. De même, les documents bureautiques produits doivent être stockés sur des serveurs de fichiers. Ces espaces sont à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit.

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, …). Aucune donnée à caractère personnel ne doit être stockée sur des postes ou périphériques professionnels.

Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.

Les medias 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 interdite.
L'utilisateur ne doit pas transmettre de fichiers sensibles à une personne qui en ferait la demande et qu'il ne connaitrait pas, même s'il s'agit d'une adresse électronique interne à la commune et au CCAS.

5.3. Usage des ressources informatiques

Seules des personnes habilitées de la commune et du CCAS d'Aucamville ont le droit d'installer de nouveaux logiciels, de connecter de nouveaux PC au réseau de la commune et du CCAS d'Aucamville et plus globalement d'installer de nouveaux matériels informatiques.

L'utilisateur s'engage à ne pas modifier la configuration des ressources (matériels, réseaux, …) mises à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes habilitées de la collectivité.

Les logiciels commerciaux acquis par la commune et le CCAS ne doivent pas faire l'objet de copies de sauvegarde par l'utilisateur, ces dernières ne pouvant être effectuées que par les personnes habilitées.

5.4. Usage des outils de communication

Les outils de communication tels que le téléphone, le fax, 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 et du fax

Le téléphone et le fax sont des moyens potentiels d'échanges de données qui présentent des risques puisque l'identité de l'interlocuteur qui répond au téléphone ou de celui qui réceptionne un fax 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 d'Aucamville. Si un doute subsiste, le numéro de téléphone de l'interlocuteur indiqué doit être vérifié.

L'utilisateur est informé qu'un journal des communications, entrantes et/ou sortantes, est accessible par le service informatique s'agissant tant de la téléphonie fixe que mobile. Les utilisateurs sont informés que les relevés de communication peuvent faire l'objet d'un contrôle.

L'utilisateur s'engage en outre à :

- prévenir la Direction générale 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 ;
- utiliser des codes d'accès (pin, verrouillage clavier et autre) différents ;
- se déconnecter de toutes applications après usage et ne pas rester connectés par défaut ;
- 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.
En cas d'absence, les utilisateurs doivent effectuer un renvoi sur le poste d'un autre utilisateur habilité à recevoir et traiter ses appels ou sur le répondeur ou sur le service d'accueil du site sur lequel il est basé.

Les surcoûts pour l'entreprise engendrés par l'utilisation de la téléphonie à des fins personnelles devront être remboursés par les utilisateurs concernés. Il s'agit tout particulièrement des appels à des numéros surtaxés et des appels depuis l'étranger ou à destination de l'étranger, au sens de la facturation téléphonique.

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

Toutefois, seule la direction pourra avoir accès aux numéros détaillés, permettant d'identifier les interlocuteurs d'un utilisateur, et seulement en cas de différend avec lui.

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 d'Aucamville.

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.

Tous les accès Internet sont tracés et enregistrés et conservés par un dispositif de filtrage et de traçabilité. Il serait donc possible pour la collectivité de connaître, pour chaque salarié, le détail de son activité sur Internet.

Ce contrôle des accès aux sites visités permet de filtrer les sites jugés indésirables, notamment des sites dangereux pour la sécurité du réseau. Il permet de détecter, de bloquer et ou de signaler les accès abusifs (en matière de débits, volumes, durées), ou les accès à des sites illicites et/ou interdits.

5.4.3. Usage de la messagerie

L'usage de la messagerie est autorisé à l'ensemble du personnel. 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.

Pour les fichiers dont le volume excède les capacités de la messagerie, les utilisateurs devront utiliser exclusivement, chaque fois que cela est rendu nécessaire, la plateforme interne « cloud.ville-aucamville.fr ».

Un usage privé de la messagerie est toléré s'il reste exceptionnel. Les messages personnels doivent comporter explicitement la mention « privé » dans l'objet. A défaut, les messages seront réputés relever de la correspondance professionnelle. Les messages marqués « privé » ne doivent pas comporter de signature d'ordre professionnel à l'intérieur du message.

L'usage des listes de diffusion doit être strictement professionnel.

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 d'Aucamville 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.

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. En présence d'informations à caractère confidentiel, de données à caractère personnel ou de données sensibles, ces vérifications doivent être renforcées ; en cas de besoin, un cryptage des messages pourra être aussi proposé par la direction informatique.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel. Les messages doivent dans ce cas être cryptés, conformément aux recommandations du responsable des systèmes d'information.

Les messages importants doivent être envoyés avec un accusé de réception ou signés électroniquement.
La forme des messages professionnels doit respecter les règles de courtoisie habituelles. La signature des courriers électroniques fait l'objet d'une forme standardisée (cf. charte graphique). Chaque utilisateur s'engage à respecter cette forme en évitant tout élément complémentaire.

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.
Ces dispositifs ont été portés à la connaissance des utilisateurs avant leur mise en œuvre.

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. Au terme de la durée de validité des certificats, toute nouvelle demande de certificat ou de renouvellement doit être validée par le responsable hiérarchique de l'agent et transmise au service informatique.
Les certificats sont révoqués lorsque l'utilisateur quitte la collectivité ou lorsqu'il ne dispose plus de l'habilitation à l'utiliser.

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. 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 robuste (8 caractères minimum, mélange de chiffres, lettres et caractères spéciaux. Il est conseillé d'éviter les prénoms des enfants, conjoints, dates de naissance …), de préférence simple à mémoriser, mais surtout complexe à deviner. Il doit être changé régulièrement et a minima tous les 6 mois. Pour des raisons de sécurité, le service informatique imposera un changement régulier des mots de passe.
L'utilisateur devra privilégier dès à présent l'utilisation du gestionnaire de mot de passe « keepass ».
Le mot de passe est strictement confidentiel. Il ne doit pas être communiqué à qui que ce soit : ni à des collègues, ni à sa hiérarchie, ni au personnel en charge de la sécurité des systèmes d'information, même pour une situation temporaire.

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. La plupart des systèmes informatiques et des applications assurent une traçabilité complète des accès et des opérations réalisées à partir des comptes. Il est ainsi possible pour la commune et le CCAS de vérifier a posteriori l'identité de l'utilisateur ayant accédé ou tenté d'accéder à des données sur le serveur au moyen du compte utilisé pour cet accès ou cette tentative d'accès. C'est pourquoi il est important que l'utilisateur veille à ce que personne ne puisse se connecter avec son propre compte. Pour cela, sur un poste dédié, 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 (ex : messagerie d'un service, guichet …).
Seules les personnes du service informatique 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.

5.7. Photographies-droit à l'image

L'image d'une personne ne peut être utilisée sans son consentement écrit. D'une manière générale, les photos que les agents sont amenés à prendre dans l'exercice de leurs fonctions ne doivent pas comporter de personnes, plaques d'immatriculation, etc … 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 d'Aucamville 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 service informatique de la commune et du CCAS d'Aucamville 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 service informatique 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 récupèrera 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

Un nouveau règlement de l'Union européenne, appelé 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 collectivité a pris en compte ces nouvelles directives.
Toute création ou modification de fichier comportant des données personnelles, doit préalablement à sa mise en œuvre, être déclarée auprès du Délégué à la Protection des données personnelles DPO de la commune et du CCAS d'Aucamville, qui étudie alors la pertinence des données recueillies, la finalité du fichier, les durées de conservation prévues, les destinataires des données, le moyen d'information des personnes fichées et les mesures de sécurité à déployer pour protéger les données. Le DPO procède ensuite aux opérations internes de modification du Registre des traitements.

Il est rappelé que l'absence de déclaration de fichiers comportant des données à caractère personnel est passible de sanctions financières.

En cas de non-respect des obligations relatives à la loi Informatique et Libertés et du Règlement Général sur la Protection des Données, le DPO serait informé et pourrait prendre toute mesure temporaire de nature à mettre fin au traitement illégal ainsi qu'informer le responsable hiérarchique de l'utilisateur à l'origine du traitement illégal.

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 d'Aucamville.

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.

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. DROIT A LA DECONNEXION

La commune et le CCAS d'Aucamville s'engagent à contribuer à une articulation optimale entre la vie personnelle et la vie professionnelle de chaque collaborateur pour l'utilisation des technologies actuelles et futures.

Les outils numériques (ordinateurs, téléphones et/ou tout support multimédia rentrant dans cette catégorie) mis à disposition des agents par la collectivité et son établissement public à des fins professionnelles sont susceptibles d'être utilisés en dehors des horaires de travail. La commune et le CCAS d'Aucamville rappellent à ses agents qu'il n'existe pas d'obligation liée à l'utilisation des outils hors des horaires indiqués dans leurs contrats de travail. Si l'utilisation des outils numériques peut être effectuée hors des horaires de travail afin d'optimiser l'accomplissement de tâches nécessitant une actualisation dans les meilleurs délais, la commune et le CCAS d'Aucamville recommandent à l'ensemble de ses agents de veiller à ne pas faire une utilisation qui porterait une atteinte manifeste à l'équilibre entre leur vie personnelle et leur vie professionnelle.

Concernant les agents en situation de télétravail, ces derniers pourront annuellement analyser avec la Direction et le service des Ressources Humaines, outre les conditions d'activité de l'emploi concerné, les plages horaires durant lesquelles la commune et le CCAS d'Aucamville pourront habituellement prendre contact avec le collaborateur.

9. 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.

10. 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 service informatique met en place toutes les mesures techniques nécessaires à son application et au contrôle de son exécution.

Cette charte annule et remplace la précédente intitulée « charte de bonne conduite pour l'utilisation de l'outil informatique, des réseaux et du téléphone » du 21 décembre 2012.

Aucamville, le 12 mars 2021

AUCAMVILLE

AUCAMVILLE
Centre Communal d'Action Sociale

RECEPISSE DE LA CHARTE DE BON USAGE DES MOYENS INFORMATIQUES ET DE TELECOMMUNICATIONS

Je soussigné (e)

Nom – Prénom : .....

Direction/Service : .....

En tant qu'utilisateur du système d'information et de communication de la ville et du CCAS d'Aucamville, déclare :

- Avoir pris connaissance de la charte de bon usage des moyens informatiques et de télécommunications
- M'engage à respecter pendant toute la durée de mes fonctions, et sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel

Fait à .....le .....

Signature du bénéficiaire, précédée de la mention « lu et approuvé »

Ce récépissé est à retourner à la direction des ressources humaines suite à sa signature