COMMUNAUTE DE COMMUNES

AIRVAUDAIS-VAL DU THOUET

33 Place des Promenades 79600 AIRVAULT

N° D2021-61

EXTRAIT DU REGISTRE DES DELIBERATIONS DU CONSEIL COMMUNAUTAIRE

Réunion Ordinaire du 29 juin 2021

L'an deux mil vingt et un le vingt-neuf du mois de juin à 18 h 30, le Conseil Communautaire de la Communauté de Communes Airvaudais-Val du Thouet, s'est réuni au nombre prescrit par la loi, à la salle des fêtes « La Jauleterie » à Assais-les-Jumeaux, régulièrement convoqué par M. Olivier FOUILLET, Président de la CCAVT.

23 présents + 1 pouvoir (24 votes) :
Membres titulaires présents :

- ✓ Commune d'Airvault : Olivier FOUILLET, Maryse CHARRIER, Viviane CHABAUTY, Jacky JOZEAU, Sylvie NOBLET-HORTET, Gaëtan GARREAU, Mattieu MANCEAU, Frédérique DAMBRINE, Frédéric PARTHENAY, Lucette ROCHER
- ✓ Commune d'Assais-les-Jumeaux : Fabrice DURAND, Jean-Claude LAURANTIN
- ✓ Commune d'Availles-Thouarsais : Daniel ROBERT
- ✓ Commune de Boussais : Jacques ROY, Gérard GIRET
- ✓ Commune d'Irais : Hélène MARSAULT
- ✓ Commune de Le Chillou : Françoise RICHARD
- ✓ Commune de Louin : Monique NOLOT
- ✓ Commune de Maisontiers : Gérard CHABAUTY
- ✓ Commune de Saint-Loup-Lamairé : Pascal BIRONNEAU, Dominique BARREAU, Alain JEZEQUEL, Micheline REAU

1 pouvoir :
✓ Dominique GUILBOT a donné pouvoir à Fabrice DURAND

Excusés : Maryse BARIGAULT, Mathias DIXNEUF, Jérôme GLORIAU, Dominique GUILBOT

Alain JEZEQUEL a été élu secrétaire de séance.

Date de la convocation : Mardi 22 juin

RESSOURCES HUMAINES
Approbation de la charte informatique

- Vu l'avis favorable du Comité Technique en date du 25 mai 2021,

Après délibération et à l'unanimité des membres présents et représentés, le Conseil Communautaire :
✓ Décide de valider la charte d'utilisation des outils informatiques ci-jointe
✓ Autorise M. le Président ou son représentant à signer tous les documents se rapportant à cette délibération.

A Airvault, le 29 juin 2021
Le Président,
Olivier FOUILLET

AR-Préfecture
079-200041416-20210707-391-DE
Acte certifié éxécutoire
Réception par le Préfet : 07-07-2021
Publication le : 07-07-2021

Pour copie conforme,
Le Président,
Olivier FOUILLET

COMMUNAUTE DE COMMUNES
AIRVAUDAIS - VAL DU THOUET
33 Place des Promenades
79600 AIRVAULT
Tél. 05 49 64 93 48

Charte d'utilisation des outils informatiques

de la

Communauté de Communes Airvaudais-Val du Thouet

et du

Centre Intercommunal d'Action Sociale Airvaudais-Val du Thouet

Validée par le Conseil Communautaire en date du : ……

Table des matières

A- Préambule

Le développement des technologies de l'information et de la communication a conduit le personnel de la Communauté de Communes Airvaudais-Val du Thouet (CCAVT)et du Centre Intercommunal d'Action Sociale Airvaudais-Val du Thouet (CIAS AVT) à utiliser dans leur travail quotidien l'outil informatique, les réseaux et les services de communication numériques pour l'exécution de leurs missions.

Le service informatique de la Communauté de Communes a ainsi mis en place différents dispositifs techniques de sécurité destinés à réduire la vulnérabilité du système d'information, pour éviter par exemple l'importation de virus, et à garantir des performances optimales des réseaux, par la mise en place de règles d'usage notamment.

Sur le plan juridique, il est par ailleurs primordial que chaque agent respecte certaines règles d'utilisation pour se prémunir d'actions susceptibles d'engager sa responsabilité personnelle, civile et/ou pénale, de répondre sur le plan disciplinaire, ou d'engager la responsabilité de la collectivité (atteintes aux droits de la personne résultant des fichiers de données à caractère personnel, atteintes aux droits d'auteur…).

La présente charte, qui se veut avant tout un document d'information et de référence, a ainsi pour objet :
- de déterminer les conditions d'utilisation des moyens ou/et des ressources informatiques mis à disposition,
- de définir les droits et obligations des personnes utilisatrices de ces outils, dans le respect des droits et libertés de chacun,
- d'informer et sensibiliser sur les risques encourus pour les prévenir, et garantir ainsi la sécurité, l'intégrité et la confidentialité des données.

Cette charte est susceptible d'être modifiée régulièrement en fonction des évolutions technologiques et réglementaires, le cas échéant. Chaque utilisateur s'engage à la respecter.

La présente charte s'applique à l'ensemble du personnel tous statuts confondus, ainsi qu'au personnel temporaire. Elle s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques de l'établissement. Tout contrat avec un prestataire extérieur devra y faire référence et comporter comme annexe la présente charte.
Dès l'entrée en vigueur de la présente charte, chaque agent de l'établissement s'en verra remettre un exemplaire. Il devra en prendre connaissance et s'engager à la respecter.

B- Conditions d'accès aux systèmes informatiques

Le droit d'accès aux ressources informatiques de la CCAVT et du CIAS AVT est conditionné par le respect des termes de cette charte dont la notification individuelle vaut acceptation pleine et entière.
Les accès informatiques sont personnels.
Ils cessent avec la disparition des raisons qui ont motivé leur attribution. Ils sont limités aux activités professionnelles définies dans le cadre de la mission de l'utilisateur.

Par ailleurs, l'étendue des ressources informatiques auxquelles l'utilisateur a accès peut être limité en fonction des besoins réels et des contraintes imposées par le partage de ces ressources avec d'autres utilisateurs.
Le droit d'accès peut être suspendu, par mesure conservatoire de l'autorité hiérarchique, si le comportement d'un utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

C- Confidentialité

Lorsque le poste de travail fonctionne en réseau, un nom de compte (login) est fourni à l'utilisateur, auquel est associé un mot de passe.

Pour être suffisamment efficace, ce mot de passe doit être strictement personnel et respecter les règles demandées par le service informatique de la Communauté de Communes. Pour des raisons de sécurité, il est recommandé de changer régulièrement ce mot de passe, conformément aux recommandations de la CNIL. Le service informatique se réserve le droit d'imposer techniquement ce changement si nécessaire.

Chaque utilisateur est responsable de l'utilisation qui est faite de son compte réseau, il lui appartient donc de ne communiquer son mot de passe à aucune tierce personne.

L'utilisateur s'engage expressément à :
- ne pas masquer sa véritable identité,
- ne pas usurper l'identité d'autrui,
- ne jamais « prêter » son compte réseau,
- signaler au service informatique toute violation ou tentative de violation suspectée de son compte réseau et, de façon générale, toute anomalie constatée.

Il faut noter que les dispositions prévues ci-dessus s'appliquent partiellement lorsque le compte réseau est par nature partagé par plusieurs agents (exemple : login générique « Accueil »).

D- Installation et utilisation des matériels et des logiciels

1°) Postes informatiques (hors tablettes numériques)

Tout utilisateur s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquence :
- de modifier le fonctionnement, le paramétrage et les caractéristiques de son poste de travail informatique (installation de nouveaux matériels, de logiciels même gratuits, modification des fichiers systèmes),
- de modifier des éléments de configuration tels que veilles animées, curseurs animés, fond d'écran, dans des limites portant atteinte aux performances du poste de travail ou de l'image de l'établissement,
- d'interrompre, même temporairement, le fonctionnement de tout système connecté au réseau (le déplacement de tout matériel informatique ou téléphonique doit être

réalisé par le service informatique ou à défaut par une personne expressément habilitée par le service informatique),
- d'accéder à des informations privées d'autres utilisateurs du réseau (en dérobant son mot de passe par exemple),
- de modifier ou détruire des informations communes (partagées par plusieurs utilisateurs) stockées sur le réseau.

Il est expressément rappelé que l'accès à des informations privées d'autres utilisateurs, leur éventuelle destruction ou modification sont des agissements pénalement sanctionnés.

L'enregistrement des travaux des utilisateurs doit être réalisé dans les espaces prévus à cet effet : répertoires du service ou d'échange sur le réseau, répertoires personnels sur son poste. Tout document situé hors de ces répertoires pourra être supprimé par les administrateurs du réseau sauf dispositifs spécifiques et/ou contraintes particulières. A noter que les données stockées en local sur les PC ne font l'objet d'aucune sauvegarde.

2°) Postes téléphoniques fixes

L'utilisation du téléphone fixe est réservée à des fins professionnelles.
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 bien sur le service d'accueil du site sur lequel il est basé.
L'usage du téléphone fixe pour des communications personnelles est toléré aux conditions qu'il soit ponctuel, qu'il concerne des appels locaux et n'entrave pas l'activité professionnelle des utilisateurs.

3°) Téléphones mobiles

Un téléphone mobile peut être mis à la disposition des utilisateurs pour un usage strictement professionnel.
À ce titre, l'utilisateur est tenu :
- d'en prendre soin et de se conformer aux prescriptions d'usage, décrites dans la notice d'utilisation fournie avec le téléphone,
- d'informer immédiatement le service informatique en cas de dysfonctionnement, de blocage, de perte ou de vol de l'équipement.

Il est rappelé que selon le code de la route, l'usage d'un téléphone par le conducteur d'un véhicule en circulation est interdit.
Si le téléphone mobile autorise une connexion à l'internet et à la messagerie, les utilisateurs devront respecter les obligations et interdictions visées aux présents points « messagerie électronique» et « Internet » ci-dessous.
A noter que toute utilisation abusive et non professionnelles pourrait faire l'objet de sanction.

4°) Logiciels

L'utilisateur ne peut installer un logiciel (qu'il soit payant ou gratuit), que ce soit par copie de cédérom, téléchargement ou autre, qu'après accord exprès du responsable du service

informatique et sous réserve d'une validation préalable d'opportunité formalisée par le directeur ou le chef de service auquel l'agent est hiérarchiquement rattaché.
Aucune copie de logiciel n'appartenant pas au domaine public (respect du droit de propriété) n'est autorisée en dehors des copies de sauvegarde. Pour information, l'utilisation et la diffusion de logiciels piratés constituent un délit passible d'amende forte et d'emprisonnement. Sa diffusion correspond à du recel.

5°) Copieurs numériques multifonctions

Du fait de leurs fonctionnalités étendues, les copieurs numériques constituent un périphérique dont la sécurité doit être assurée comme celle des postes de travail informatiques. Dès lors que des informations à protéger transitent par ce type d'appareil, l'ensemble des recommandations et réglementations relatives aux systèmes d'informations s'appliquent.
Lors de la numérisation de documents, les utilisateurs doivent s'assurer que la destination des fichiers ainsi générés est accessible aux seules personnes habilitées à accéder à ces informations.

Les utilisateurs doivent s'abstenir de reproduire, copier, diffuser des pages web, images, photographies, textes ou toutes autres créations protégées par le droit d'auteur.
Une sensibilisation est faite aux utilisateurs afin :
- d'éviter l'impression systématique de mails (et notamment en couleur) ou de documents en version provisoire,
- d'utiliser la fonction « aperçu » avant d'imprimer,
- d'utiliser le mode d'impression couleur, uniquement pour les documents contenant des visuels le nécessitant.

6°) Utilisation à des fins personnelles

L'utilisation des équipements informatiques et téléphoniques de la CCAVT et du CIAS AVT est limitée à un usage professionnel.

L'utilisation à titre privé est tolérée mais doit être occasionnelle et sous réserve qu'elle ne perturbe pas l'activité professionnelle.

L'encadrement pourra proposer à l'autorité territoriale de sanctionner tout utilisateur ayant une utilisation abusive des moyens informatiques ou téléphoniques.

7°) Signature électronique et certificat

Certains utilisateurs, dans le cadre de leurs fonctions, sont amenés à utiliser des certificats de signature électronique pour signer des documents et/ou s'authentifier pour accéder à des services sécurisés.
Ces certificats sont nominatifs et non-cessibles, ils sont constitués de 3 éléments indissociables :
- les informations concernant l'identité du titulaire, son organisation, sa fonction, la période de validité du certificat et l'identité de l'autorité de certification qui l'a généré,

- la clé privée,
- la clé publique.

L'utilisateur doit ainsi veiller à garder confidentiel le code saisie (clé privée) lors de la signature avec son certificat.

Les certificats ont une durée de validité limitée (1,2 ou 3 ans). Toute nouvelle demande de certificat ou de renouvellement doit être validé par le responsable hiérarchique de l'agent et transmis au service informatique.

Les certificats seront révoqués lorsque leur utilisateur quitte la collectivité ou ne dispose plus de l'habilitation à l'utiliser.

8°) Travail à distance

Pour rappel, l'employeur est responsable de la sécurité des données à caractère personnel collectées en tant que responsable du traitement, y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique, mais dont il a autorisé l'utilisation pour accéder aux ressources informatiques de l'entreprise.

Cette charte informatique s'applique également pour le personnel en travail à distance.

En cas d'utilisation d'un ordinateur personnel, la collectivité demande aux agents de ne stocker aucun document professionnel sur leur poste.

Il est également demandé aux agents de s'assurer que celui-ci est suffisamment sécurisé :

- antivirus, pare-feu,
- et mise à jour régulière du système d'exploitation et des logiciels utilisés.

E- Loi Informatique et Libertés

En application des dispositions de la loi Informatique et Libertés n°78-17 du 6 janvier 1978 modifiée et de la directive européenne 95/46/CE du 24 octobre 1995, relative à la protection des données personnelles et à la libre circulation de ces données, la CCAVT et le CIAS AVT respectent les règles légales de protection de ce type de données.

Ils garantissent notamment aux membres de son personnel :

- de n'utiliser les données à caractère personnel les concernant que pour les strictes finalités pour lesquelles elles sont collectées (ouverture de compte d'accès, contrôles techniques définis dans la partie I « Administration du système informatique et contrôles techniques » de la présente charte…),
- de lui communiquer les finalités et la destruction des informations enregistrées et leur durée de conservation, laquelle ne peut en tout état de cause excéder ce qui est nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou traitées,
- de lui garantir un droit d'accès et de rectification aux données le concernant.

Il est tout autant impératif que chacun des membres du personnel s'astreigne aux règles ci-dessus édictées.

Cette obligation s'impose tout particulièrement si par l'utilisation qu'il fait du matériel informatique mis à sa disposition, il devait être amené à créer, utiliser ou traiter tout fichier contenant des informations nominatives directes ou indirectes.
La création, l'utilisation ou le traitement de tels fichiers, faite en dehors d'un usage professionnel, doit être proscrite.
Plus précisément, en cas de constitution de fichiers, l'utilisateur veillera en particulier :

- à respecter les procédures préalables auprès de la CNIL, en avisant pour ce faire son autorité hiérarchique et le service informatique,
- à procéder à l'information préalable des personnes concernées, quant à la finalité et les destinataires du traitement de ces informations,
- à n'effectuer auprès des personnes concernées aucune collecte d'informations concernant notamment leurs opinions politiques, syndicales, philosophiques ou religieuses, de leur origine, de leur orientation sexuelle, le leur âge, de leur patronyme, de leur état de santé, de leur apparence physique, de leur handicap ou de leur appartenance ou de leur non appartenance, vraie ou supposée, à une ethnie ou une race.

Ces dispositions s'appliquent également aux moyens de communication électroniques (messagerie). Ainsi, il est interdit de faire circuler, d'échanger, de fusionner des fichiers nominatifs. Toutefois, l'envoi de messages comportant des informations nominatives (à distinguer des fichiers nominatifs) entre professionnels habilités à traiter de l'information individuelle nominative pour les besoins professionnels, est autorisé sous réserve du respect des obligations déontologiques générales, et notamment du secret professionnel.

F- Déontologie -Éthique

Chaque utilisateur s'engage à respecter les règles de la déontologie informatique dans l'esprit des principes généraux fixés par le statut des fonctionnaires. Les règles de déontologie et d'éthique professionnelles s'appliquent à l'ensemble des documents produits par les utilisateurs.
Cela concerne les notes manuscrites, les documents imprimés, mais également les fichiers et les messages électroniques.

G- Messagerie électronique

Les outils de messagerie apportent de nouvelles possibilités et des facilités qui peuvent aller à l'encontre des usages établis. Dans ce cadre, une liste des principales règles à respecter doit être indiquée.

1°) Comportement vis-à-vis de la hiérarchie

La transmission d'information par la messagerie doit respecter les procédures de contrôle, de validation, d'autorisation.

Il est donc rappelé que les usages habituels du « en copie » sont directement applicables par la zone correspondante dans l'en-tête du message.

Il est souhaitable de systématiquement s'interroger sur les destinataires à mettre en copie du message, et notamment son responsable hiérarchique. En effet, tout autant qu'assurer une information pertinente de ses supérieurs, il s'agit de ne pas excessivement alourdir leur messagerie.

2°) Contenu des messages électroniques

Les utilisateurs disposent d'une boîte aux lettres permettant de recevoir et d'émettre des messages électroniques uniquement professionnels.

Les règles générales d'utilisation :
- l'auteur doit utiliser la signature mise en service par le service informatique de la CCAVT. A défaut (ou en complément), il devra s'identifier en faisant figurer en bas du message son nom, sa fonction, son service, éventuellement son numéro de téléphone et le logo de la structure,
- la transmission d'information par la messagerie doit respecter les procédures internes de contrôle, de validation, d'autorisation. Il est souhaitable de mettre systématiquement en copie de message important son responsable et le responsable du destinataire,
- il est recommandé de vérifier la liste des destinataires avant l'envoi de tout message et d'utiliser la fonction copie cachée (Cci) afin de ne pas rendre le contenu de ces listes accessibles à tous,
- en cas d'absence, doit être activé un message automatique d'absence indiquant la date de retour prévue et éventuellement la personne ou le service à joindre en cas d'urgence,
- les fichiers joints ne doivent pas dépasser 10 Mo. Pour des transferts supérieurs à 10 Mo, il est conseillé l'utilisation de sites internet comme https://wetransfer.com/.
- pour les transmissions de fichiers en interne, il est recommandé de communiquer le chemin d'accès au fichier sur le réseau dans son message, plutôt que de l'envoyer en pièce jointe.

Le principe veut que les messages émis et reçus par le salarié sur la messagerie mise à sa disposition par son entreprise soient présumés avoir un caractère professionnel. A ce titre, l'employeur peut librement les consulter à condition que ceux-ci n'aient pas été identifiés par le salarié comme étant personnels (Cass. Soc. 26.06.12, n° 11-15310). S'ils sont identifiés comme tels, l'employeur pourra toutefois les consulter mais seulement en présence du salarié (Cass. Soc. 16.05.13, n° 12-11866).

Dans ce cadre, la collectivité se réserve le droit d'effectuer des contrôles dans des cas graves de mauvaise utilisation (la liste suivante n'étant pas exhaustive) :
- envoyer ou recevoir délibérément des informations et données dont le contenu et la forme peuvent nuire à la collectivité,
- envoyer des informations confidentielles sur l'organisation, le personnel et les élus de la collectivité,
- envoyer des messages pouvant engager la responsabilité contractuelle de la collectivité.

Les mêmes dispositions s'appliquent également pour l'utilisation de boîtes aux lettres professionnelles génériques.

3°) Engagement vis-à-vis des tiers

Un message électronique peut être une preuve ou un début de preuve. Ainsi, en matière commerciale, une preuve peut être apportée par tous les moyens possibles et il y a contrat dès lors que les parties ont donné leur accord sur la chose et sur le prix.

Il est donc rappelé que toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent à la messagerie. Il est donc obligatoire de transmettre pour validation à un responsable tout message qui aurait valeur contractuelle ou qui serait l'expression d'une décision administrative.

4°) Comportement/Actes illicites

Il est interdit aux utilisateurs de stocker, transférer ou diffuser des documents proscrits par la loi, et notamment les documents à caractère raciste, négationniste ou pornographique.
Un agent ne peut être tenu pour responsable s'il reçoit, à son insu, de tels messages mais il lui est imposé de les détruire. II ne doit donc pas en solliciter l'envoi en participant à des groupes de discussion, ou en consultant des sites, dont le caractère est proscrit, qui pourrait enregistrer ses coordonnées.

5°) Conservation des messages

Il est conseillé de :

- conserver tous les messages, envoyés ou reçus, qui peuvent avoir une valeur contractuelle,
- supprimer rapidement tous les messages volumineux et sans valeur contractuelle,
- purger régulièrement les anciens messages devenus inutiles (supérieurs à deux ans par exemple).

La durée de conservation des sauvegardes est définie au point 7 ci-après.

6°) Sécurité

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

Des outils ont été mis en place pour se prémunir contre ce type d'attaque : tout message infecté détecté par le système de protection sera éradiqué par réparation ou suppression automatique selon les possibilités. Toutefois, il est impossible de garantir un niveau de sécurité total.

Il est donc nécessaire de respecter les précautions simples décrites ci-dessous :
- ne pas ouvrir les messages suspects (non sollicités, ayant un objet douteux, provenant d'un émetteur inconnu ou comportant des liens ou des pièces jointes bizarres). Il est indispensable de les signaler au service informatique pour analyse ou les supprimer directement,

- ne pas répondre à une demande d'informations confidentielles (mots de passe, code PIN, coordonnées bancaires, etc.) reçue par mail, ceci directement ou en complétant un formulaire en ligne. Jamais le service informatique ne vous demandera ce type d'information par email,
- en cas de doute sur l'expéditeur d'un message, contactez son interlocuteur pour vérifier qu'il est à l'origine du message et ainsi éviter les phénomènes d'usurpation d'identité,
- prévenir immédiatement le service informatique, dans le cas de réception de messages non sollicités récurrents ou manifestement illicites.

En outre, et afin d'assurer un niveau de sécurité maximum, il est strictement interdit de désactiver les systèmes de protection du poste du travail.

7°) Utilisation de la messagerie électronique à des fins personnelles

Il est considéré que tout message reçu ou envoyé à partir du poste de travail mis à la disposition de l'utilisateur revêt par principe un caractère professionnel.
L'utilisation de la messagerie à des fins personnelles, lorsqu'elle est rendue nécessaire par les impératifs de la vie courante et familiale, est tolérée si elle n'affecte pas le trafic normal de la messagerie professionnelle.

Le message qui comportera la mention expresse ou manifeste de son caractère personnel dans l'en-tête, bénéficiera du droit au respect de la vie privée et du secret des correspondances. Cependant, l'utilisateur doit être informé de ce que toute activité numérique, comme l'utilisation de la messagerie électronique, laisse des traces et est nécessairement mémorisée. En particulier, l'ensemble des messages reçus ou envoyés est conservé sur un dispositif de sauvegarde, pour une durée ne pouvant excéder douze mois.

L'utilisateur doit être informé que, pour des raisons de sécurité, d'organisation ou de gestion de l'encombrement du réseau, le service informatique peut mettre en place des dispositifs d'analyse de messages ou des dispositifs visant à limiter la taille ou le volume des messages échangés. La mise en place de ces dispositifs n'ayant pas pour objet le contrôle individuel des utilisateurs, la confidentialité des messages sera respectée.

Si des anomalies étaient détectées, des mesures de contrôle individuel par poste peuvent être mises en place après information préalable de l'agent concerné et de sa hiérarchie.

H- Internet : accès aux sites Web non professionnels

1°) Consultation des sites Web

Seuls ont vocation à être consultés les sites Internet ayant un lien direct et nécessaire avec l'activité professionnelle et présentant une utilité au regard des missions et des fonctions à exercer.

Une consultation ponctuelle et raisonnable des sites Internet dont le contenu n'est pas contraire à l'ordre public et qui ne mettrait pas en cause les intérêts et les règles éthiques et déontologiques de la CCAVT et du CIAS AVT, est admise.

Un dispositif de filtrage des accès pourra être mis en place par le service informatique pour permettre à chacun de disposer d'un accès performant mais restreint aux sites professionnels dans les plages horaires d'activité régulière, et d'un accès potentiellement moins performant mais ouvert aux sites non professionnels à des plages horaires dédiées.
(Exemple : entre 12 h 30 et 13 h 45 et entre 17 h 45 et 8 h 30).

L'utilisateur s'engage expressément à respecter les lois et règlements en vigueur sur le territoire français et notamment de manière non limitative ceux régissant le fonctionnement des services en ligne, le commerce, la vente à distance, la protection des mineurs, le respect de la personne humaine et de la vie privée, la propriété intellectuelle.

Il s'interdit de stocker, diffuser ou rendre accessible de quelque façon que ce soit tout message dont contenu serait contraire notamment à la dignité humaine, à l'ordre public et aux bonnes mœurs, ou constituant une incitation à la pédophilie, à la haine raciale, au meurtre, au terrorisme, au proxénétisme, au trafic de stupéfiants, à la contrefaçon notamment par fournitures de moyens illicites, au piratage informatique, ou susceptible de constituer une atteinte à la sécurité nationale.

Dans la mesure où des utilisations contrevenant aux règles ci-dessus énoncées, sont susceptibles d'engager la responsabilité administrative, civile et/ou pénale de la CCAVT et/ou CIAS AVT, outre bien évidemment celle de l'utilisateur, le service informatique se réserve la possibilité d'exercer un droit de regard sur l'usage de l'internet par le personnel, ce dont l'utilisateur déclare expressément prendre connaissance et accepter.

2°) Usage des blogs, forums et réseaux sociaux

A l'instar des sites Internet, une utilisation ponctuelle et raisonnable des blogs, des forums et des réseaux sociaux (Facebook, Twitter, LinkedIn, Viadeo, etc.) est admise.

Il est toutefois important de rappeler que tous les agents sont soumis au devoir de réserve. A ce titre, l'utilisation des médias sociaux, au sein et en dehors de la collectivité, doit être limitée aux échanges d'ordre privé.

En conséquence, exception faite des services dont c'est la mission, aucun agent n'est autorisé à s'exprimer au nom de la CCAVT et/ou du CIAS AVT sans autorisation expresse de la Direction.

Par ailleurs, la publication d'informations confidentielles, de commentaires diffamatoires contre des collègues ou l'institution, ou toute autre information concernant l'activité de la CCAVT et/ou du CIAS AVT sur des forums, des blogs ou des réseaux sociaux est susceptible d'entraîner des poursuites (disciplinaires, pénales ou civiles selon le type d'infraction).

Concernant les comptes utilisés sur les réseaux sociaux, il est expressément interdit de créer un profil susceptible de représenter un service ou une fonction de la CCAVT et/ou du CIAS AVT, afin de permettre à chacun d'utiliser ce média à titre privé, sans que les propos échangés ne puissent être considérés comme liés de près ou de loin à l'activité exercée au sein de la structure.

I- Administration des systèmes d'information et contrôles techniques

Le service informatique doit assurer le bon fonctionnement des réseaux et des moyens informatiques.
Il a le droit de prendre toutes dispositions nécessaires pour assumer cette responsabilité, tout en respectant la déontologie professionnelle.

Il peut ainsi effectuer des contrôles techniques sans information préalables de l'utilisateur :
- soit dans un souci de sécurité du réseau et/ou des ressources informatiques : pour des nécessités de maintenance et de gestion technique, l'utilisation des services et notamment des ressources matérielles et logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment dans le respect des règles relatives à la protection de la vie privée et au respect des communications privées ;
- soit dans un souci de vérification que l'utilisation des moyens informatiques, de la messagerie et de télécommunication reste conforme aux règles édictées par la présente charte.
En particulier, le service informatique dispose d'outils permettant d'analyser tout ce qui transite par celui-ci, notamment :
- les connexions au réseau (identifiants, dates et heures de connexion...),
- les fichiers stockés sur les serveurs (format, date, taille...),
- les connexions Internet (identifiants de connexion, sites visités, volumes de données transférées, dates et heures de connexion...),
- les consommations téléphoniques sur les mobiles.

Le service informatique est assujetti au devoir de réserve et est tenu de respecter la confidentialité des informations auxquelles il pourrait avoir accès dans le strict cadre de ses missions, conformément à l'obligation de raison professionnelle.

En raison de la nécessité de pouvoir procéder aux contrôles ci-dessus exposés, l'utilisateur reconnaît accepter expressément les mesures de contrôle mises en œuvre ci-avant exposées, étant rappelé que le service informatique a l'obligation de préserver la confidentialité des informations privées qu'il serait amené à connaître dans ce cadre.

<u>Cas exceptionnels</u>

Pour assurer la continuité du service public, le service informatique, sur demande de l'autorité territoriale (Direction uniquement) peut accéder :
- à la messagerie d'un utilisateur absent en respectant la législation en vigueur et sous certaines conditions : il est notamment interdit à quiconque de prendre connaissance d'un message professionnel ayant pour objet « Personnel » ou « Confidentiel », sans l'autorisation expresse de l'utilisateur (qu'il en soit l'auteur ou le destinataire),
- aux fichiers pendant l'absence des utilisateurs ; toute mesure devant être prise pour empêcher l'accès aux données identifiées comme personnelles sur les outils de travail.

Par ailleurs, pour des raisons exceptionnelles de sauvegarde de la sécurité, tous les messages professionnels pourront être ouverts par le service informatique sur demande écrite de l'autorité territoriale.

J- Droits et devoirs des utilisateurs

1°) Principes généraux

Les utilisateurs doivent :
- appliquer les recommandations de sécurité inscrites dans la présente charte,
- respecter les règles de bon usage afin d'éviter des opérations qui pourraient avoir pour conséquence de nuire à la collectivité,
À ce titre, ils :
- disposent d'un droit d'accès strictement personnel et incessible,
- contribuent à la sécurité informatique, en signalant tout dysfonctionnement ou toute anomalie des ressources qu'ils utilisent,
- utilisent les logiciels dans le respect des règles relatives à la propriété intellectuelle et des droits d'auteur. Ils ne doivent pas reproduire et/ou ne pas diffuser des données soumises à un droit de copie qu'ils ne détiennent pas,
- ne doivent pas introduire de « ressources extérieures » matérielles ou logicielles qui pourraient porter atteinte à la sécurité du système d'information et de communication,
- effectuent des sauvegardes à échéances régulières pour les fichiers autres que ceux déjà sauvegardés automatiquement sur le réseau.

L'utilisation des moyens informatique et télécom doit se limiter à un usage professionnel dans le cadre des missions de service public de la collectivité. Elle doit être réalisée de manière loyale et responsable par tous les utilisateurs.
L'usage à titre personnel doit rester exceptionnel et particulièrement modéré dans sa fréquence et sa durée et ne pas nuire au bon fonctionnement du service.

2°) Respect de la confidentialité des données

a) Droit d'accès aux fichiers

Droit d'accès, c'est-à-dire, le droit d'être informé et de demander l'accès aux données personnelles que la collectivité traite.

Les utilisateurs sont amenés à gérer, du fait de leurs compétences et dans le cadre de leurs missions, des fichiers dont il est nécessaire de garantir la confidentialité : fichiers d'usagers des services, dossiers individuels et bulletins de paie des utilisateurs, etc.
Ils doivent ainsi veiller :
- à respecter l'intégrité et la confidentialité des données, tant pour la collecte, le traitement et la communication interne et externe des données,
- à ne pas copier ni sauvegarder les fichiers professionnels sur support amovible autres que ceux fournis par la collectivité,
- ne pas collecter des données qui, en raison de leur contenu, contreviendraient aux lois et règlements en vigueur.

Une gestion des droits d'accès est mise en place pour interdire l'accès aux fichiers confidentiels à toute personne autre que le ou les gestionnaires desdits fichiers.

Les utilisateurs s'engagent par ailleurs à ne pas prendre connaissance d'informations appartenant à autrui sans son accord, à ne pas communiquer à un tiers de telles informations ou des informations non publiques auxquelles il peut accéder, mais dont il n'est pas propriétaire.

L'utilisateur est averti que les données enregistrées sur les serveurs de fichiers (lecteurs réseaux, etc.) sont partagées avec d'autres utilisateurs, notamment les agents de son service. L'enregistrement de données à caractère personnel et confidentiel sur les serveurs de fichiers mis à disposition est donc proscrit.
Les règles de secret professionnel, de déontologie, d'obligation de réserve et de devoir de discrétion s'imposent concernant les informations présentes sur le réseau et les messages électroniques professionnels.

b) La protection des données personnelles informatiques

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 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. Les utilisateurs peuvent exercer ces droits auprès de Monsieur le Président responsable du traitement de la collectivité et également auprès du DPD (prestataire retenu par le CDG conformément à la délibération n°D2020-105 en date du 8 décembre 2020 de la CCAVT).

3°) En cas de départ d'un utilisateur

Tout utilisateur, lors de la cessation de son activité au sein de la collectivité, perd son habilitation à utiliser les systèmes d'information internes.
Il doit :
- restituer tous les matériels mis à sa disposition,
- effacer de son poste de travail tous ses éventuels fichiers et données privés.

Il ne peut effectuer une copie de son travail professionnel qu'après autorisation écrite de son supérieur hiérarchique dûment habilité.

Les éventuels répertoires personnels ainsi que les données de messagerie des utilisateurs situés sur le serveur seront obligatoirement supprimés par le service informatique, en tout état de cause dans un délai maximum d'un mois après son départ.

K- Sanctions applicables

La loi et les textes réglementaires définissent les droits et obligations des personnes utilisant les moyens informatiques (articles 226-16 à 226-24 du Code pénal portant sur les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques, articles 323-1 à 323-7 du Code pénal portant sur les atteintes aux systèmes de traitement automatisé de données).

Il est rappelé qu'en cas d'atteinte à l'un des principes protégés par la loi, la responsabilité administrative, pénale et/ou civile de l'agent ainsi que celle de la collectivité est susceptible d'être recherchée.

Par ailleurs, toute infraction aux règles internes décrites dans le présent document peut entrainer des sanctions disciplinaires.

L- Opposabilité de la charte

La présente charte est rendue opposable dès sa notification à chaque utilisateur valant acceptation entière de ses termes.

Le Président,
M. Olivier FOUILLET

Déclaration de l'utilisateur

Je soussigné(e) *Nom, Prénom* ……, certifie avoir pris connaissance de la présent charte et m'engage à m'y conformer sans restriction.

Je certifie également avoir pris connaissance de mon droit d'accès et de rectifications aux informations personnelles détenues par la Collectivité, conformément aux articles 38 à 43 de la loi n°78-17 du 6 janvier 1978 modifiée.

Mention manuscrite « Lu et approuvé » :……

Lieu, date :……

Signature :

Fait en double exemplaire : un exemplaire à conserver par l'utilisateur, un exemplaire à remettre à la Collectivité.

----------✂----------

Déclaration de l'utilisateur

Je soussigné(e) *Nom, Prénom* ……, certifie avoir pris connaissance de la présent charte et m'engage à m'y conformer sans restriction.

Je certifie également avoir pris connaissance de mon droit d'accès et de rectifications aux informations personnelles détenues par la Collectivité, conformément aux articles 38 à 43 de la loi n°78-17 du 6 janvier 1978 modifiée.

Mention manuscrite « Lu et approuvé » :……

Lieu, date :……

Signature :

Fait en double exemplaire : un exemplaire à conserver par l'utilisateur, un exemplaire à remettre à la Collectivité.