

NOTE DE SERVICE

du 24 juin 2024

OBJET : CHARTE DES USAGES NUMÉRIQUES

De : Benoit BELLEC – Directeur Général des Services

À : Tous les agents + affichage sur tous les sites

Numéro : 2024.03

Cette note a pour objet de présenter les enjeux (sécurité informatique, protection des données, ...) de la nouvelle charte des usages numériques de CCA, qui y est annexée. Elle concerne tous les agents à des degrés divers.

CONTEXTE

Tout organisme amené à traiter des données personnelles doit mettre en place une charte informatique. Il s'agit d'un document qui précise comment les ressources informatiques internes (système d'information) doivent être utilisées.

La dernière version de la charte informatique de CCA datait de 2018 et les nouveaux usages (télétravail, réseaux sociaux), et l'évolution de la réglementation (RGPD, ...) ont rendu nécessaire sa mise à jour.

Aussi une nouvelle version a été proposée par la DSI, la DRH et le service communication et a été approuvée en Comité Social Territorial le 26 mars 2024, puis validée en conseil communautaire le 30 mai 2024.

La charte a vocation à s'appliquer tant aux agents qu'aux élus à qui des matériels et services sont mis à disposition.

QU'EST-CE QU'UNE CHARTE DES USAGES NUMÉRIQUES ?

Il s'agit d'une action de la Politique de Sécurité des Systèmes d'Information adoptée en conseil communautaire fin 2022. En effet, de nombreuses règles de la charte sont motivées par des enjeux de sécurité informatique.

Elle traite de l'utilisation des e-mails, du matériel informatique, des réseaux sociaux, de l'application du RGPD (Règlement Général sur la Protection des Données), etc.

La charte fixe également des limites quant à l'utilisation de ces ressources, pour maîtriser les risques en matière de cyber sécurité ou de détournement de données personnelles.

Il s'agit donc d'un ensemble de règles qui permettent de donner un cadre à l'utilisation de ces ressources informatiques.

LA COMMUNICATION ET SENSIBILISATION DES AGENTS

La diffusion de la charte, par l'envoi de la présente note de service à l'ensemble des agents, son affichage sur les sites et sa remise à tous les nouveaux arrivants, sera complétée par l'intervention de la Direction des Systèmes d'Information dans les réunions de service, à la demande des responsables de service et/ ou des directeurs de pôle, sur les questions de sécurité informatique en général, sur les « bonnes pratiques », ce qui permettra un temps d'échanges sur tout sujet en lien avec la DSL.

De plus, des organismes extérieurs (Centre de Gestion, Mégalis,...) sont mobilisés pour des interventions sur les questions de sécurité informatique : un programme de sensibilisation / formation sera communiqué prochainement.

D'ici là, je vous invite à lire attentivement cette nouvelle Charte des Usages numériques, et à vous y conformer.

La Direction des Systèmes d'Information se tient à votre disposition pour toute question relative à sa compréhension ou son application.



Le Directeur général des services,
Benoit BELLEC

ANNEXE : Charte des Usages Numériques de CCA

CHARTE des USAGES NUMERIQUES

Cette charte s'applique à l'ensemble des moyens de communication et des ressources informatiques et numériques mis à disposition des agents et élus de Concarneau Cornouaille Agglomération, quelles que soient les formes sous lesquelles ils sont exploités.

Une charte, pour quoi faire ?

- ▷ Sécuriser notre système d'information, protéger chaque utilisateur
- ▷ Clarifier les droits, les devoirs et les responsabilités de chacun
- ▷ Adopter des comportements de sécurité et de sobriété

Vous êtes responsable du bon usage des équipements et ressources mis à votre disposition. Utilisez ces ressources de façon rationnelle, loyale et conforme aux obligations légales afin d'en éviter la saturation ou le détournement abusif à des fins personnelles. L'utilisation des ressources doit être uniquement réalisée dans le cadre de vos missions professionnelles.

SOMMAIRE :

- MON MATERIEL
- MES ACCES
- DONNEES PERSONNELLES
- PARTAGE DE RESSOURCES
- MESSAGERIE ELECTRONIQUE
- TELEPHONIE
- SOBRIETE NUMERIQUE ET VIVRE ENSEMBLE
- TELETRAVAIL
- DROITS ET DEVOIRS DE DECONNEXION
- RESEAUX SOCIAUX

ANNEXES :

- Mesures prises en cas d'infraction
- Cadre réglementaire
- Missions des Administrateurs

MON MATÉRIEL



- ▷ **Je prends soin et respecte l'intégrité du matériel mis à disposition.** Je suis responsable du matériel prêté et garant de sa bonne utilisation et de son entretien pour optimiser sa durée de vie.
- ▷ **Je respecte les différentes procédures d'utilisation (allumage, fermeture, ...)** mises à sa disposition. Vidéoprojecteurs, visio, ... et utilise les matériels de protection fournis avec le matériel (housses, ...)

Le matériel est mis à disposition à des fins professionnelles

Même s'il existe une tolérance, cette règle doit être respectée notamment pour des raisons de sécurité, et de coût. En cas d'abus (utilisation trop personnelle d'internet, du téléphone ou de la messagerie), la Direction Générale sera informée.

A noter : la DSI n'intervient pas sur le matériel personnel de l'agent ou de l'élu.

Tout matériel mis à disposition à un agent / élu précis doit être restitué à la DSI au départ de l'agent ou à la fin du mandat de l'élu. Si ces outils sont prêtés avec des accessoires de protection, ils doivent être restitués en même temps (sacoche, protection écran, étui à rabat...).

INTERDITS

- ▷ **Modifier le fonctionnement, le paramétrage et les caractéristiques de son poste de travail informatique (modification des composants matériels, de logiciels même gratuits, modification des fichiers systèmes...)**
- ▷ **Modifier le lieu d'implantation du matériel informatique ou téléphonique (sauf matériel nomade)**
- ▷ **Modifier ou détruire des données qui pourraient impacter le bon fonctionnement du système d'exploitation.**
- ▷ **Réaffecter du matériel à un autre agent/ élu. Seule la DSI est habilitée à le faire.**
- ▷ **Acheter du matériel informatique ou téléphonique. Tous les achats de matériel informatique ou téléphonique sont réalisés par la DSI ou à minima faire l'objet d'un accord express de sa part.**
- ▷ **Prêter ou mettre à disposition ces équipements à d'autres personnes.** Ces matériels sont mis à disposition pour un usage strictement professionnel et ne doivent en aucun cas être utilisés par des personnes ne faisant pas partie de la collectivité et/ou n'ayant pas signé la présente charte.

FOIRE AUX QUESTIONS

Une utilisation hors les murs ou par des tiers ? Lorsque ces matériels sont utilisés à l'extérieur (réunions hors des locaux de la collectivité), **vous en assurez la garde et la responsabilité.** Niveaux de surveillance et de confidentialité renforcés et veiller à ce que des tiers non autorisés ne puissent accéder à ces moyens ni les utiliser.

Télétravail ? Soyez vigilant à l'accès par des personnes de votre entourage.

Dysfonctionnement, blocage, perte ou vol des matériels ?

1. J'informe immédiatement la DSI.
2. J'assiste CCA, dans toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

En cas d'incident, CCA prend en charge les dommages subis par les biens de toute nature mis à disposition de l'agent / de l'élu. Par ailleurs, les dommages causés aux tiers sont pris en charge par CCA s'ils résultent directement de l'exercice de ces missions / fonctions ou s'ils sont causés par des biens mis à disposition par CCA. Si les dommages résultent d'une faute personnelle détachable du service, vous êtes responsable.

MES ACCÈS

Vos identifiants : l'accès aux ressources informatiques repose sur l'utilisation d'un nom d'utilisateur (parfois aussi nommé « compte », « login » ou « identifiant ») associé à un mot de passe que vous seul devez connaître. À votre arrivée dans la collectivité la DSI vous communique un mot de passe à usage temporaire que vous devez modifier à la première connexion. La DSI pilote la politique de mots de passe et impose une typologie de mots de passe (complexité, nombre de caractères, ...) et une fréquence de renouvellement, consignes obligatoires à respecter dans le cadre de la politique de sécurité des systèmes d'informations (PSSI).

Ces identifiants préservent la confidentialité des informations professionnelles. Ils sont individuels et confidentiels. Vous êtes responsable de l'utilisation qui peut en être faite.

La DSI peut néanmoins réinitialiser les mots de passe, si l'utilisateur est absent et si c'est nécessaire à la continuité du service public.

Vos droits d'accès au réseau :

Des droits sont mis en place afin de vous permettre d'avoir accès uniquement aux dossiers vous concernant.

Bon réflexe !



- ▷ Je différencie les mots de passe dans ma vie professionnelle et personnelle.
- ▷ Quand je m'absente de mon poste de travail (même momentanément), je verrouille le poste
(via la combinaison de touches Ctrl + Alt + Suppr ou touche Windows + L).
NB : verrouillage automatique programmé au bout d'une certain temps d'inutilisation de l'ordinateur.
- ▷ Je reçois un visiteur qui souhaite se raccorder au réseau ? Le réseau Wifi public est en libre accès.

Pour qu'un prestataire accède au réseau interne, un accord préalable de la DSI est nécessaire (anticipez ! faites un ticket) : le prestataire se verra affecter un compte le temps de l'opération.

INTERDITS

- ▷ Télécharger, installer, utiliser ou contourner l'utilisation d'un logiciel pour lequel la collectivité n'a pas acquis de licence. Seuls les administrateurs informatiques sont habilités à installer de nouveaux logiciels, y compris des logiciels libres.
- ▷ Copier un logiciel pour l'utiliser sur un autre poste ou en dehors de son lieu de travail.
Des droits de reproduction existent également pour les œuvres littéraires, musicales, photographiques, audiovisuelles qui ne doivent en aucun cas être téléchargées reproduites ou diffusées sans autorisation de l'auteur ou du propriétaire des droits d'exploitation.
- ▷ Connecter sans autorisation, à un poste ou au réseau, un équipement étranger à la collectivité et susceptible de provoquer des dysfonctionnements ou d'introduire des virus informatiques.
Exemple : un smartphone personnel par exemple connecté en USB sur un ordinateur professionnel.

Toute connexion d'un nouveau matériel doit se faire avec l'autorisation de la DSI.

Les intervenants extérieurs ne doivent utiliser que le Wifi public.

- ▷ **Connecter à votre poste informatique des équipements personnels : smartphones, tablettes, lecteurs MP3, montres connectées, clefs USB personnelles, disques durs externes, etc.**
Il existe des solutions pour les transferts des gros fichiers permettant de se passer des clefs USB, sources de virus.
- ▷ **Désactiver le logiciel de protection antivirus ou d'en modifier le paramétrage.**
Le logiciel antivirus vous avertit en cas de détection de virus et vous devez en informer la DSI immédiatement
- ▷ **Installer des applications sur votre smartphone sans l'accord de la DSI.** Limiter leurs usages au contexte professionnel.
- ▷ Certaines catégories de sites internet sont bloquées (ex : jeux d'argent ...).

Bon réflexe !

Vous constatez une anomalie du système d'information ou de son utilisation ? Informez sans délai la DSI.

DONNÉES PERSONNELLES

ZOOM RGPD - Règlement Général sur la Protection des Données.

Vous êtes utilisateurs ou créateurs de fichiers contenant des données personnelles

> Assurez-vous auprès de votre responsable hiérarchique ou du délégué à la protection des données (DPD) de la régularité du traitement (contact DPD : protection.donnees@cdg29.bzh)



- ▷ Je déclare tout nouveau traitement de données personnelles auprès du Délégué à la Protection des Données : protection.donnees@cdg29.bzh
- ▷ Je communique ma véritable identité, n'usurpe pas l'identité d'une autre personne pour accéder à ses informations.
- ▷ Je respecte les données d'autrui.

INTERDIT

- ▷ Altérer les données et accéder à des informations appartenant à d'autres utilisateurs, sans leur autorisation
- ▷ Modifier ou détruire des ressources connectées au réseau sans autorisation des administrateurs ou d'un supérieur hiérarchique ou à minima sans s'être assuré que ces ressources ne sont pas utilisées par d'autres utilisateurs.
- ▷ De répertorier des données personnelles sans déclaration de traitement auprès du DPD.

Une donnée, c'est : un nom, un prénom, un numéro de sécurité sociale, une adresse, une fiche de paie, un n° d'immatriculation, un n° de CAF, un n° de téléphone,

CCA se réserve le droit de sanctionner disciplinairement l'agent en infraction, et peut l'exposer à des poursuites judiciaires.

TRAITEMENT DE VOS DONNÉES PERSONNELLES

Elles sont à la fois protégées et tracées.

- ▷ Les informations issues des matériels utilisant le réseau, la date, l'heure de connexion, la durée de connexion, les traces de navigation, etc.) seront conservées sur *6 mois maximum*.
- ▷ Vous bénéficiez de droits (accès, rectification, effacement, limitation, portabilité, opposition) relatifs à l'utilisation de leurs données et avez le droit d'introduire des réclamations auprès de l'autorité de contrôle qu'est la Commission nationale de l'Informatique et des Libertés (CNIL).

Traçabilité des connexions et des accès :

Des dispositifs de connexion gérés par la DSI conservent des traces des connexions effectuées depuis les postes de travail fixes ou mobiles. Les informations enregistrées sont les suivantes :

- ▷ **Les connexions téléphoniques**, à savoir la liste des appels (appelant, sortant, durée), sans enregistrement des contenus des appels servent principalement à des fins statistiques, leur durée de conservation est *6 mois maximum*.
- ▷ **Les photocopies**, à savoir la liste des volumes d'impression et de numérisation par code utilisateur et/ou de service.
- ▷ **Les arrivées et départs des agents** transmis par le service RH à la DSI : cette dernière est chargée de créer et supprimer les comptes et les droits.
Les comptes Windows et de messagerie sont désactivés au départ des agents et élus pendant une durée de 1 mois puis supprimés.
- ▷ **Sur les serveurs** – réseau interne : l'identifiant de l'utilisateur, l'horodatage de l'ouverture ou fermeture de session - *6 mois maximum*

Contrôle des connexions vers Internet : Le nom ou l'adresse réseau du poste de travail / identifiant de l'utilisateur / adresse IP du serveur de destination / pages Web demandées / horodatage / autorisation ou le blocage de l'accès (par exemple sites web relevant des catégories : armes, sexe, drogues, alcools, violence, terrorisme) / raisons de l'éventuel blocage / Durée de conservation : *6 mois maximum*

Contrôle d'accès aux bâtiments de CCA

L'accès à certains locaux de la collectivité est contrôlé par des automatismes permettant ainsi de limiter les entrées de personnes étrangères aux services à certaines plages horaires. Les utilisateurs et/ou services nécessitant un accès sont dotés de badges permettant l'ouverture des portes en dehors des plages horaires d'ouverture au public.

La traçabilité de l'accès aux locaux est conservée (max. 3 mois) par le logiciel de gestion d'accès, à savoir la liste des badges utilisés sur les lecteurs de badges.

Ces informations pourront être communiquées à des tiers :

- ▷ Pour se conformer à des obligations légales ou pour obéir à des injonctions judiciaires,
- ▷ Pour protéger et défendre ses droits, notamment ses droits de propriété,
- ▷ Pour protéger les intérêts des agents et des élus.

INTERDIT

- ▷ **Céder ou prêter son badge ou celui du service à une personne non autorisée.**

Vous êtes doté d'un badge, sachez que chaque utilisation donne lieu à un enregistrement horodaté dans le respect de la législation en vigueur.

PARTAGE DE RESSOURCES



- ▷ **Vous disposez d'espaces de stockage sur les réseaux informatiques de la collectivité ou hébergés chez nos partenaires : bases de données, serveurs de messagerie, serveurs de fichiers, etc.**

La DSI sauvegarde les informations stockées sur les serveurs uniquement : la sauvegarde des fichiers stockés sur votre poste de travail n'est pas réalisée.

Bonne pratique

- ▷ **Je conserve sur les serveurs uniquement les données directement liées à mon activité professionnelle. Si j'ai quelques fichiers personnels, ils doivent être enregistrés sur le disque local de mon PC dans un dossier identifié comme « Personnel » ou « Privé ». Pour la messagerie : l'utilisateur se crée un dossier nommé « personnel » pour y stocker ses informations ou données personnelles.**

INTERDITS

- ▷ **Interdit de sauvegarder des fichiers professionnels sur des supports personnels ou sur des sites extérieurs à la collectivité.**
- ▷ **Interdit d'utiliser, même temporairement, l'infrastructure informatique de CCA pour copier transférer ou traiter des données personnelles.**

Une utilisation à titre privé des moyens de communication est admise, dès lors qu'elle est raisonnable et qu'elle ne nuit pas au bon fonctionnement du service.

Le réseau informatique



Le réseau informatique est un **espace commun** dans lequel chaque utilisateur doit se retrouver. Pour un partage efficient de l'information, cela nécessite que les fichiers et données y soient déposées selon des **règles communes à tous**.

Une réorganisation du réseau informatique est actuellement en cours et sera proposée par la DSI et formalisée dans le cadre d'une note de service ; chaque agent est tenu de la respecter.

Nommage des fichiers

Objectif : que chacun à CCA puisse disposer à tout instant du document dont il a besoin. La règle de nommage est basée sur la structure suivante de nom de fichier :

AbreviationServiceRedacteur_MotClef_AbreviationTypologieDocument_date_Version

3 exceptions

- La commande publique : n° du marché_Mot-clef ou Objet du marché
- Les commissions : AbréviationCommissionsDate_AbréviationTypologieDocument
- Les délibérations : DELIB_n° de la délibération_MotClef



- ▷ **Se référer à la note de service n°2018-11 sur la dématérialisation des procédures et la gestion électronique des documents : règles de nommage et plans de classement**

MESSAGERIE ELECTRONIQUE :

Seules les personnes habilitées au sein de la DSI administrent et ont accès aux paramétrages des boîtes aux lettres. L'accès au contenu peut aussi être autorisé pour les administrateurs sous certaines conditions (dépannages, absences ...) (voir annexe 3 : administrateurs).

Bon à savoir : Les échanges électroniques avec des tiers ont la même **valeur juridique** que les échanges écrits. Un message électronique peut donc être une preuve ou un début de preuve, engageant l'utilisateur ou CCA, au même titre qu'un courrier écrit.



- ▷ **Je conserve tous les messages, envoyés ou reçus, qui peuvent avoir une valeur contractuelle ou une valeur juridique pertinente** (exemples : engagement sur une prestation, conseil statutaire sur un dossier sensible, procédure marché public...). Si les messages n'ont pas ces types de valeurs, évitez d'encombrer vos boîtes mails en les conservant.
- ▷ **En mon absence, je prends les dispositions nécessaires pour assurer la continuité du service public** (ex : message d'absence de messagerie indiquant les contacts des suppléants). Toute communication de mots de passe personnels est proscrite.
- ▷ **Je prends des dispositions pour ne plus recevoir de messages à caractère personnel sur ma messagerie professionnelle.**
De façon exceptionnelle, et par nécessité de continuité de service public, longue maladie, ou départ définitif de CCA, et sur la demande de la direction générale (DGS + DGA), CCA pourra être amenée à accéder à la messagerie de l'utilisateur en son absence. Idem pour les messages téléphoniques. Les messages identifiés comme personnels ne seront pas consultés.
- ▷ **Je partage mon agenda de messagerie**

INTERDITS

- ▷ Diffuser des informations confidentielles relatives à CCA à ses usagers, cocontractants et partenaires ou aux agents sauf si la conduite des dossiers ou le droit à l'information le requiert.
- ▷ Ouvrir une pièce jointe ou cliquer sur un lien contenu dans le message, dont je ne suis pas absolument certain de la provenance et de l'innocuité.
- ▷ Utiliser à titre professionnel de comptes de messagerie non gérés par la collectivité.
- ▷ Mettre en place une redirection vers ma boîte personnelle

TÉLÉPHONIE



- ▷ J'utilise les n° d'appels internes (raccourcis) sans passer par le standard
Pour éviter d'engorger le standard et appels par raccourcis non facturés.
- ▷ Je me réfère à l'annuaire téléphonique et aux organigrammes régulièrement mis à jour. Ils sont accessibles sur l'Intranet.
- ▷ Quand je suis absent(e), je fais un renvoi vers une assistante ou un collègue ou mets un message d'absence sur son répondeur.
La DSI est à votre disposition pour vous conseiller sur les outils à privilégier.
- ▷ J'ai un téléphone mobile et me déplace à l'étranger pour raisons professionnelles, je préviens la DSI.

SOBRIETÉ NUMÉRIQUE et VIVRE ENSEMBLE



- ▷ Je diffuse mes messages internes via l'intranet, en m'appuyant sur la chargée de communication interne
- ▷ J'évite de joindre des pièces jointes volumineuses et je privilégie l'envoi des liens des documents enregistrés sur le réseau plutôt que l'envoi par pièce jointe.
- ▷ Je supprime régulièrement les mails qui n'ont pas de valeur et vide régulièrement la corbeille.
- ▷ Je veille à ce que la diffusion des messages soit limitée aux seuls destinataires concernés.
- ▷ Je limite mon consentement préalable à recevoir un message de type commercial, newsletter, abonnement à des listes de diffusion.
- ▷ Je reste courtois dans mes échanges électroniques. L'envoi d'un mail ou d'un ticket ne dispense pas de règles minimales de politesse.

Dans certains cas (communication sensible, complexe ou nombre d'interlocuteurs) il est préférable d'utiliser des modes de communication autres que le mail pour échanger (réunion, visio, téléphone, ...) pour gagner en efficacité et compréhension réciproque.

La DSI est à votre disposition pour vous conseiller sur les outils à privilégier.

Imprimantes et photocopieurs



- ▷ **J'évite l'impression de mails** ou de documents en version provisoire
- ▷ **J'utilise la fonction « aperçu » avant d'imprimer un document** et vérifie sa mise en page, pour optimiser et limiter l'usage des feuilles
- ▷ **J'utilise le mode d'impression noir et blanc**, sauf pour les documents contenant des visuels le nécessitant.
- ▷ **Je n'imprime pas de documents personnels**
- ▷ **J'utilise le mode recto-verso et le mode « brouillon » pour utiliser moins d'encre**

La DSI assure un suivi des consommations des copieurs et peut être amenée à préconiser la suppression de certains copieurs. Les imprimantes personnelles sont quant à elles proscrites sauf cas très particuliers soumis à l'accord de la Direction générale.

- ▷ **J'éteins les matériels en place** (ordinateurs, imprimantes, mobiles...) lors de déplacements, congés, en rendez-vous et à la fin de la journée de travail.
- ▷ **Je ferme les applications** avant toute mise hors tension des appareils.
- ▷ **Avant l'organisation d'une réunion**, je réfléchis à la meilleure forme à proposer (présentiel / visio) au regard des échanges d'information nécessaires mais également du « coût » du déplacement.

TÉLÉTRAVAIL

CCA met à disposition du télétravailleur :

- ▷ Un **ordinateur portable** que le télétravailleur s'engage à utiliser dans le respect de la présente charte.
- ▷ Une **solution de téléphonie adaptée**
- ▷ Une **assistance informatique à distance**

En cas de panne ou de mauvais fonctionnement des équipements mis à disposition le télétravailleur doit avant tout vérifier le bon fonctionnement de sa connexion internet auprès de son opérateur. Une fois cette étape validée et en cas de dysfonctionnement persistant, le télétravailleur peut en aviser la DSI. L'équipement informatique est couvert par le contrat d'assurance de CCA.

- ▷ **CCA ne participe pas aux frais d'abonnements personnels nécessitant la connexion à l'internet ou l'usage des terminaux personnels tels que mobiles ou téléphones fixes.**



- ▷ **Je respecte les mêmes règles de confidentialité, d'usage des équipements et logiciels que lorsque je travaille en présentiel.**
- ▷ **Je dispose d'une connexion ADSL d'au moins 8 mégabits par seconde descendant.** Pour vérifier le débit de connexion : <https://www.speedtest.net>.
- ▷ **Je suis joignable autant qu'en présentiel : je procède à un transfert de mes appels téléphoniques.**

DROITS ET DEVOIRS DE DÉCONNEXION

CCA souhaite favoriser une articulation optimale entre la vie personnelle et la vie professionnelle de chaque agent. **Vous pouvez être amenés à recevoir des messages en dehors de votre temps de travail (mails voire appels téléphoniques).**

- ▷ **Les mails quelle que soit leur heure d'envoi (par exemple par un agent travaillant en soirée), n'appellent en aucun cas une réponse immédiate, sauf cas particulier (astreinte ou urgence signalée) ;**
- ▷ **Vous devez couper les renvois vers les téléphones personnels ou professionnels si vous n'êtes pas en activité ;**
- ▷ **Il peut être prévu, par accord entre les supérieurs et les collègues et le télétravailleur, de communiquer sur les plages où le télétravailleur est joignable (par exemple en indiquant ces horaires sur la messagerie Yaziba).**

RÉSEAUX SOCIAUX

Les médias sociaux regroupent les différentes activités qui intègrent l'interaction sociale et la création de contenu. Les plateformes sociales sont des **véritables espaces publics, visibles et consultables par tous**. Tout le monde peut propager vos idées en republant un contenu écrit, vidéo ou audio instantanément.

- ▷ **Je suis impliqué personnellement sur tout ce que je publie ou retransmet** (partage, "like", commentaire, etc....).
- ▷ **Je demeure soumis aux obligations de réserve, de discréction et de secret professionnel.** Je fais preuve de mesure dans mes propos (tant sur les réseaux CCA que mes réseaux personnels) afin de ne pas porter atteinte à l'image ou à la considération de CCA., des élus, agents et partenaires
- ▷ **Je limite l'usage des réseaux sociaux à un usage strictement professionnel durant le temps de travail.**

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.

Charte validée en Comité Social Territorial le 26 mars 2024 et en conseil communautaire le 30 mai 2024

ANNEXE 1 - MESURES PRISES EN CAS D'INFRACTION / GESTION DES ABUS - RESPONSABILITÉS

Une procédure disciplinaire et/ ou pénale, pouvant aller jusqu'au licenciement pour faute grave, en fonction de la gravité et/ou des conséquences des faits sur le préjudice subi par l'employeur, pourra être engagée envers l'utilisateur ou l'administrateur suite à une utilisation non conforme à cette charte ou des législations en vigueur.

La Direction Générale se réserve notamment le droit, en cas d'une utilisation contraire à cette charte, d'interdire l'utilisation d'Internet et/ou de la Messagerie à titre privé à une personne ou à l'ensemble des utilisateurs.

En cas du non-respect de la présente charte ou de la législation en vigueur, outre la mise en œuvre de sanctions disciplinaires à l'encontre des utilisateurs, CCA se réserve le droit d'appeler en garantie l'utilisateur ou l'administrateur pour les dommages et intérêts qu'elle aura dû éventuellement régler à un tiers en raison d'agissements non conformes. Ceux-ci sont donc informés qu'ils peuvent engager leur responsabilité civile et/ou pénale.

ANNEXE 2 – LE CADRE RÉGLEMENTAIRE

Chaque agent est personnellement responsable de son utilisation des moyens informatiques. À ce titre, il peut voir sa responsabilité individuelle engagée du fait d'une mauvaise utilisation.

La présente annexe a pour objectif d'informer les utilisateurs des principaux textes législatifs et réglementaires définissant les droits et les obligations des personnes utilisant les moyens informatiques. Il ne s'agit en aucun cas d'une liste exhaustive.

- Le Code Pénal, notamment ses articles 323-1 à 323-7 relatifs à la fraude informatique.
- Le Code de la propriété intellectuelle qui reconnaît les logiciels comme œuvre de l'esprit et, à ce titre, les protège sans nécessité de dépôt ou d'enregistrement.
- Loi n°83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale, imposant notamment les obligations de réserve, de discrétion et de secret professionnel des agents publics.
- Loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, qui a notamment pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'emploi de l'informatique et d'encadrer l'utilisation des données à caractère personnel dans les traitements informatiques.
- Loi n°94-665 du 4 août 1994 modifiée, relative à l'emploi de la langue française.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril, dit Règlement Général sur la Protection des Données (RGPD) qui constitue le texte de référence en matière de protection des données à caractère personnel.
- Décret n°85-397 du 3 avril 1985 modifié relatif à l'exercice du droit syndical dans la fonction publique territoriale

Télétravail :

- Article 133 de la loi n° 2012-347 du 12 mars 2012 dite Loi Sauvadet, modifié, a consacré la possibilité pour les agents publics (fonctionnaires ou non) d'exercer leurs fonctions dans le cadre du télétravail.
- Décret n°2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique.

Réseaux sociaux :

- Déclaration des droits de l'homme et du citoyen de 1789
- Code pénal : Article R621-1
- Loi du 29 juillet 1881 modifiée relative à la liberté de la presse (art. 32 et 33)

ANNEXE 3 - MISSIONS DES ADMINISTRATEURS

Les administrateurs informatiques, membres de la DSI, assurent la sécurité et le fonctionnement des moyens techniques, dans le cadre de la Politique de Sécurité des Systèmes d'Informations validée en conseil communautaire le 8 décembre 2022. De par leurs missions ils peuvent être amenés à accéder à des données personnelles et confidentielles (boîte aux lettres des utilisateurs, accès aux dossiers ...). Ils ont une obligation de confidentialité et ne peuvent pas divulguer d'informations dont leur mission leurs donneraient accès.

Dans ce cadre la confidentialité des données sera respectée (devoir de réserve et de secret professionnel des administrateurs). C'est un contrôle individuel des agents dans le but de protéger les réseaux et de garantir le bon usage de ces outils.

De plus, l'ensemble des informations est conservé sur un dispositif de sauvegarde, dans la limite de la durée légale de conservation.

Ils assurent et maintiennent la sécurité du système : Notamment par l'installation du système d'exploitation de mon ordinateur et des mises à jour nécessaires (mission exclusive des administrateurs). Ils sécurisent les postes de travail par des procédures de verrouillage automatique de sessions, et surveillent le système d'information par des logiciels régulièrement mis à jour et des pare-feux, ils sécurisent l'informatique mobile par des codes de déverrouillage, ils limitent les flux réseau au strict nécessaire, sécurisent les serveurs et les sites web, sauvegardent régulièrement et encadrent les développements informatiques.

Ils m'accompagnent dans l'utilisation de mes moyens informatiques et de communication : Notamment par la formation, l'assistance pour résolution de problèmes techniques, et l'information des contraintes de service liées au maintien du bon fonctionnement des moyens informatiques et de communication (ex : interruption de service, maintenance, ...).

Ils interviennent sur mes outils en cas de force majeure : Ils peuvent avoir momentanément accès aux ressources informatiques indispensables à la poursuite de l'activité du service, si possible après m'avoir informé(e), et à l'exclusion de l'accès à mes répertoires, fichiers et messages clairement identifiés ou expressément signalés comme lieu de stockage privé.

Ils analysent les éléments sources de problèmes techniques : La prévention et la résolution de problèmes techniques autorisent les administrateurs à analyser un certain nombre d'éléments relatifs aux flux de trafic et aux volumes stockés et notamment les :

- ▷ fichiers stockés (format, taille, date...)
- ▷ ressources matérielles et logicielles
- ▷ connexions au réseau (identifiants, dates et heures de connexions...)
- ▷ échanges via le réseau
- ▷ connexions internet (identifiants et horaires de connexion, volumes de données transférées, ...)
- ▷ messages stockés (fréquence, taille des fichiers transmis...)

Les administrateurs métier : ce sont des agents dans les services opérationnels qui ont des droits leur permettant de gérer les droits d'accès aux « logiciels métiers ».