Charte informatique

de la Communauté de Communes Cœur de Loire

Applicable au 01/01/2025

COMMUNAUTÉ DE COMMUNES CŒUR DE LOIRE
4 place Georges Clemenceau - BP 70 - 58203 Cosne-Cours-sur-Loire
Tél : 03 86 28 92 92 | contact@coeurdeloire.fr
coeurdeloire.fr

TABLE DES MATIÈRES

Le Président de la Communauté de Communes Cœur de Loire,

Vu le Code Général des Collectivités Territoriales et établissements publics,

Vu la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,

Vu la Loi n° 83-634 du 13 juillet 1983 modifiée portant dispositions statutaires relatives à la Fonction Publique Territoriale,

Vu la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,

Vu le décret n° 2011-219 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne,

Vu les articles 323-1 à 323-7 du Code Pénal,

Vu les articles L335-1 à 335-10 du Code de la Propriété Intellectuelle,

Vu le Code du Travail,

Vu l'avis favorable du Comité Social Territorial du 22/10/2024,

Vu la délibération du Conseil Communautaire en date du 7/11/2024,

AVANT-PROPOS

Tous s'accordent à dire que l'informatique est l'invention du siècle dernier, elle a révolutionné notre manière de vivre et de travailler. Automatisation, diffusion d'informations, intelligence artificielle : nous vivons dans un environnement où les pratiques évoluent chaque minute.

Ces différents outils technologiques offrent aux agents de la collectivité une grande ouverture vers l'extérieur. Cette ouverture apporte des améliorations, des aides, des performances importantes si l'utilisation de ces outils technologiques est faite à bon escient et selon certaines règles.

A l'inverse, une mauvaise utilisation de ces outils peut avoir des conséquences extrêmement graves. En effet, ils augmentent les risques d'atteinte à la confidentialité des données (agents et usagers), de mise en jeu de la responsabilité de l'utilisateur, d'atteinte à l'intégrité et à la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vols de données…). C'est ainsi que chaque jour, des personnes mal intentionnées volent notamment des codes de carte bleue, en se connectant aux serveurs des sites marchands. Les risques pour la collectivité sont donc identiques.

L'objectif est donc clair : protéger nos données et celles de nos usagers. Cela passe par la rédaction, l'approbation et le respect de cette charte par tous. Cette charte vise à sensibiliser et informer sur l'utilisation des outils technologiques. Elle traite de l'intégralité des outils numériques : internet, WIFI, messagerie, outils bureautiques, logiciels, téléphone, smartphone, etc.

Attention : elle ne vise pas à retirer des outils professionnels indispensables à l'exercice quotidien de chacun.

Au-delà, l'intérêt est de pouvoir communiquer à chacun un guide des bonnes pratiques mais aussi de protéger et alerter sur les responsabilités que nous avons tous et cela dans un environnement professionnel fait de libertés contraintes.

PREALABLE LEXICAL

La présente charte s'adresse à l'ensemble des agents de la Communauté de Communes Cœur de Loire. Elle constitue un code de bonne conduite attaché aux usages des Systèmes d'Information que l'on nommera « SI ».

On désignera de façon générale sous le terme « ressources du SI » :

- Les moyens informatiques mis à disposition,
- L'accès aux outils de badgeage et de contrôle des accès aux bâtiments,
- Les logiciels informatiques et industriels à usage professionnel,
- L'accès au réseau filaire et WIFI (données et voie) mis à disposition par la Communauté de Communes ;
- L'accès distant aux ressources de la collectivité via Internet et les portails pour ceux disposant des droits d'accès comme par exemple TeamViewer, Office 365, intranet…
- Les services internet mis à la disposition des utilisateurs sur leur ordinateur ou même sur leur téléphone.

La mention « utilisateurs » comprend toutes les personnes ayant accès ou utilisant les ressources du Système d'Information quel que soit leur lieu de travail à la Communauté de Communes Cœur de Loire.

On désignera par « services internet », l'ensemble des moyens d'échanges numériques : sites internet, messagerie, échanges de fichiers numériques…

QUI DONNE LES ACCES AUX RESSOURCES INFORMATIQUES ?

La rapidité du système informatique passe par l'utilisation responsable de chacun, elle en garantit la Sécurité.

Les droits d'accès à un utilisateur (agent, stagiaire…) ne pourront être donnés qu'après signature de la présente charte.

Les droits d'accès sont soumis à l'autorisation préalable de la Direction Générale des Services (DGS), des Responsables de Pôles ou de la Direction des Ressources Humaines.
Les ressources du SI sont accessibles pendant les heures de travail autorisées et validées par la Direction Générale.

L'équipe du service informatique de la collectivité assure une disponibilité optimale de ces ressources mais ne peut être tenue responsable d'accidents indépendants de sa volonté.

Les droits d'accès sont retirés lors de la cessation d'activité (fin de contrat, départ à la retraite…), révisés en cas de changement de poste. Ils peuvent être suspendus en cas de violation de la présente charte ou de transgression à la loi (responsabilité pénale). Cette violation peut entraîner des sanctions disciplinaires.

QUELLES SONT LES RESSOURCES INFORMATIQUES MISES A DISPOSITION ?

La collectivité met à disposition de chaque utilisateur, en fonction de ses missions, des outils lui permettant de pouvoir les accomplir. Les outils étant adaptés pour chacun, l'utilisateur ne doit pas, sans l'accord du service informatique :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Connecter ou déconnecter du réseau les outils informatiques et de communications,
- Déplacer l'équipement informatique, sauf s'il s'agit d'un « équipement nomade » : ordinateur portable, tablette, surface…
- Nuire au fonctionnement des outils informatiques et de communications.

GUIDE DE BONNES PRATIQUES

CONNEXION / DECONNEXION

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte nommé communément "login" ou identifiant, fourni à l'utilisateur (agent, stagiaire…) lors de son arrivée dans la collectivité.

Un mot de passe associé à cet identifiant de connexion est donné, et doit être modifié par l'utilisateur dès sa première connexion.

Les moyens d'authentification sont personnels et confidentiels.

Le mot de passe doit être composé de 8 caractères minimum combinant chiffres, lettres et caractères spéciaux.

Il ne doit comporter ni le nom, prénom ni l'identifiant d'ouverture de la session de travail.

Le mot de passe des sessions informatiques est renouvelé au moins 2 fois par an. L'initialisation est réalisée par le service informatique.

Pour des raisons de responsabilité, l'utilisateur s'engage à ne pas communiquer son mot de passe et à ne pas prêter ses identifiants à un tiers (sauf raison de service préalablement validée par le Responsable de Service). Il est entièrement responsable des opérations réalisées à partir de son compte.

L'utilisateur s'engage à utiliser les systèmes d'information dans le cadre de son activité professionnelle au sein de la collectivité territoriale. Toutefois, l'usage raisonnable à des fins personnelles est toléré pendant les heures de repas.

Il est demandé à chaque utilisateur de ne pas quitter son poste de travail sans avoir fermé sa session ou l'avoir verrouillée.

MESSAGERIE

IDENTIFICATION

La collectivité héberge sa messagerie via Office 365. Tout utilisateur à qui une messagerie professionnelle est créée, doit lors de sa première utilisation changer le mot de passe.

Le mot de passe doit être composé de 8 caractères minimum combinant chiffres, lettres et caractères spéciaux. Il ne doit comporter ni le nom, prénom ni l'identifiant d'ouverture de la session de travail.

BONNES PRATIQUES REDACTIONNELLES

Afin d'éviter la surcharge informationnelle, il est recommandé à tous les utilisateurs de :

- S'interroger sur la pertinence de l'utilisation de la messagerie électronique professionnelle par rapport aux autres outils de communication disponibles ;
- S'interroger sur la pertinence des destinataires du courriel (donner la bonne information, au bon interlocuteur, au bon moment).

IDENTIFICATION PRECISE DES DESTINATAIRES D'EMAILS

Les destinataires de chaque email sont identifiés clairement et distingués des personnes en copie pour information. Les destinataires (les agents dont les noms figurent dans le champ « A ») sont les agents qui doivent engager une action suite au message. Si d'autres agents doivent être tenus informés du message, ils sont mis en copie.

UTILISATION DES FONCTIONS « REPONDRE A TOUS » ET « TRANSFERER »

La fonction « Répondre à tous » est utilisée avec modération, seulement lorsque la réponse apporte une information utile aux participants à une conversation.

La fonction « Transférer » est utilisée avec discernement, seulement lorsqu'elle est nécessaire à l'activité professionnelle du destinataire, de manière à ne pas encombrer les boîtes mails.

LIBELLE DE L'OBJET DES MESSAGES

Les agents sont invités à appliquer le principe : « un message, un objet ». L'objet des messages est spécifié clairement et de manière concise dans le champ « objet », par efficacité et afin d'en faciliter l'archivage.

Lorsqu'un email appelle une réponse très rapide, cela est spécifié explicitement à la fois dans le titre et le corps de l'email. De manière générale, les mentions « Urgent » ou « TTU » dans les titres des emails comme le marqueur « Importance haute » sont réservés aux cas qui correspondent à des urgences objectives.

STRUCTURATION DES MESSAGES

Les messages sont structurés, concis, clairs et aérés et doivent comporter des paragraphes afin d'en faciliter la lecture et la compréhension. Sauf exception, leur longueur ne devrait pas excéder un espace équivalent à celui de la fenêtre d'affichage dans Outlook. Si une longue description technique est nécessaire, il est recommandé de privilégier l'utilisation d'une pièce jointe.

Il convient de faire preuve de respect, de courtoisie et de politesse lors des échanges par emails.

Pour partager des documents, permettre à plusieurs collègues de les modifier et éviter la multiplication des mails, les agents sont invités à utiliser OneDrive.

Pendant leurs congés, les agents utilisent la fonction « réponses automatiques » pour orienter leurs correspondants vers les collègues en charge de l'intérim de leurs postes et à contacter en cas d'urgence.

FONCTIONNEMENT

USAGE PERSONNEL

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée, elle ne vaut pas autorisation complète. La messagerie reste un outil professionnel.

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel dans l'objet du message, bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel. La collectivité s'interdit d'accéder aux messages identifiés comme « personnel » dans l'objet de la messagerie de l'agent ou dans un dossier de messagerie identifié comme « personnel ».

TELECHARGEMENT PIECES JOINTES

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes (clefs USB, disques durs…). C'est-à-dire soumis à l'autorisation préalable des Responsables de service.

Les agents peuvent consulter leur messagerie Office 365, à distance, via un navigateur. Les fichiers qui seraient copiés sur un ordinateur personnel doivent être effacés dès que possible pour éviter toute problématique de confidentialité.

Un utilisateur ne doit pas usurper l'identité d'une autre personne en utilisant, par exemple, la signature numérique d'un collègue, ceci afin d'éviter toute incompréhension ou responsabilité en cas de pratiques frauduleuses.

CONTENU DES MESSAGES

Les règles d'éthique professionnelle, de déontologie, d'obligation de réserve, de devoir de discrétion en usage dans les différentes professions exercées au sein de la Communauté de Communes Cœur de Loire s'appliquent à l'ensemble des documents informatiques produits et stockés par les utilisateurs.

Les utilisateurs de la messagerie devront veiller à mettre en copie ou à faire suivre à leur hiérarchie (ou à leurs collaborateurs) les messages qui le justifient. Tout courrier électronique engageant la collectivité – de quelque manière que ce soit – doit respecter les règles de délégation de signature en vigueur ; il est recommandé à l'utilisateur, en cas de doute, de solliciter l'avis de son responsable, qui jugera de l'action à engager.

Chaque utilisateur fait preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier.

CONTINUITE DU SERVICE PUBLIC

En cas d'absence d'un agent et afin de garantir la continuité du service public, le service informatique peut, ponctuellement transférer un message électronique à caractère exclusivement professionnel (avec Office 365, en cas d'utilisation de cette procédure, le mot de passe de l'utilisateur devra être réinitialisé). Ce message, est alors transféré à la demande du supérieur hiérarchique. Le supérieur hiérarchique n'a pas accès aux autres messages de l'agent. L'agent concerné est informé dès que possible de la liste des messages qui ont été transférés.

En cas d'absence prolongée ou prévisible (congés, maladie…) d'un utilisateur, supérieure à 15 jours, le responsable de service peut demander au service informatique, le transfert des messages reçus. Si l'agent est remplacé durant cette période, l'accès à sa messagerie sera bloqué pour permettre à l'utilisateur remplaçant de poursuivre les missions de service public. L'utilisateur remplaçant n'accèdera toutefois pas aux courriels personnels tolérés.

Dans un but de prévention, il est rappelé qu'un agent absent n'a pas à accéder à ses mails professionnels. En ce sens, un utilisateur peut se voir bloquer sa messagerie professionnelle, ce principe fera l'objet d'une étude individuelle, réalisée par la Direction Générale, les Responsables de Pôles et la Direction des Ressources Humaines.

La collectivité dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spams). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres.

AGENDA

Office 365 permet à chacun d'avoir accès à une messagerie, un agenda et divers applicatifs, notamment bureautiques.

Cet outil a été choisi pour sa facilité d'utilisation et de communication entre tous. Collaboratif, il permet de communiquer des informations en quelques clics.

Partage d'agenda

Il est demandé à chaque utilisateur disposant d'un compte sur Office 365 de gérer directement leur agenda sur cet outil par facilité et gain de temps. Par exemple, lors des prises de rendez-vous, cela permet de voir si les utilisateurs sont déjà occupés.

Afin de faciliter la circulation de l'information, il est demandé à chaque utilisateur de partager son agenda avec son responsable, et cela afin qu'il puisse suivre l'activité de chacun.

WEB

Tous les sites internet identifiés en catégorie « risque pénal » ou « contenu adulte » ou « risque de sécurité » sont interdits à la navigation à la Communauté de Communes Cœur de Loire.

La collectivité dispose d'un logiciel de filtrage, permettant, en fonction des missions de chacun de filtrer les contenus accessibles.

Ce logiciel permet d'améliorer la sécurité et la rapidité du réseau.

Les sites internet identifiés en catégorie « jeux en ligne », « achats » ou « réseaux sociaux » sont interdits pendant les horaires de travail, sauf pour les utilisateurs qui ont des besoins inhérents à leur poste. En cas de blocage d'un site et si besoin, l'utilisateur pourra solliciter son responsable pour validation préalable avant l'intervention du service informatique.

La navigation sur des sites catégorisés en risque pénal entraine la responsabilité juridique de la collectivité. Pour améliorer la sécurité et éviter les tentatives de piratage, un outil de collecte de données est mis en place. Les données de connexion sont conservées pendant 6 mois.

REGLES DE SAUVEGARDE

La collectivité, selon sa politique de sécurité définit la liste des espaces sauvegardés et la périodicité de sauvegarde. L'utilisateur veillera à respecter la politique de sauvegarde et d'archivage de la collectivité.
Les documents seront enregistrés dans les espaces sauvegardés afin de garantir la sécurité des données contre leur perte de disponibilité. Le service informatique a mis à disposition des espaces selon les habilitations de chaque utilisateur. L'utilisateur doit stocker et enregistrer ses documents dans ses espaces dédiés.
D'autres alternatives telle que la sauvegarde de fichiers professionnels sur des sites (gmail,..) n'est pas autorisée.
L'utilisateur ne doit pas enregistrer de document personnel dans ses espaces.

TELEPHONE

La collectivité met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et/ou mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure limitée aux cas d'urgence.

Des restrictions d'utilisation par les agents des téléphones fixes sont mises en place en tenant compte de leurs missions. La collectivité s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

La collectivité s'interdit d'accéder à l'intégralité des numéros appelés via l'autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, le service informatique, sur demande de la Direction Générale des Services, se réserve le droit d'accéder aux numéros complets des relevés individuels.

RESEAUX SOCIAUX

Les sites internet identifiés en catégorie « réseaux sociaux » sont interdits pendant les horaires de travail, sauf pour les agents qui ont des besoins inhérents à leur poste de travail (validation préalable de la Direction Générale des Services, Responsables de Pôles ou Direction des Ressources Humaines).

Il est rappelé que les utilisateurs sont soumis dans le cadre de leur fonction, mais aussi en-dehors, au devoir de réserve, de discrétion et secret professionnel, conformément à la loi n° 83-634 portant droits et obligations des fonctionnaires. En cas de transgression, des sanctions disciplinaires seront appliquées.

UTILISATION DES MATERIELS INFORMATIQUES ET TELEPHONIQUES

Le retrait des matériels nomades (tablettes, ordinateur portable, surface…), se fait auprès du service informatique. L'utilisateur doit renseigner une attestation dès qu'un matériel nomade, un téléphone portable ou smartphone lui est remis. Ce document acte la remise de l'équipement.

Il en assure la garde et la responsabilité.

Il doit informer la Direction Générale des Services en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. L'agent détenteur est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements. Le retour du matériel est remis contre signature, dans un état d'usure habituel.

En cas de dégradation à la restitution, l'agent détenteur recevra un titre de recettes calculé sur la valeur neuve dépréciée selon le tableau ci-dessous :

Années	**Pourcentage valeur du neuf**
De 0 à 1 an	80%
De 1 à 2 ans	60%
De 3 à 4 ans	40%
De 4 à 5 ans	20%

REGLES D'USAGE HORS DE LA COLLECTIVITE

NOMADISME

Est défini comme nomadisme le fait qu'un utilisateur doive se déplacer physiquement à l'extérieur de la collectivité avec son matériel informatique.

Afin de sécuriser les données du système d'information, la collectivité demande à l'utilisateur nomade de respecter méticuleusement les règles de sécurisation du poste de travail de la présente charte et lui demande également de se protéger physiquement et d'être attentif aux situations à risque lors de ses déplacements (vol, compromission de matériel et d'informations, fuites, indiscrétions…).

Enfin, l'utilisateur est tenu d'éviter d'utiliser le réseau wifi public afin de maîtriser l'accès aux flux réseaux utilisés sur son poste de travail et de prévenir son service informatique en cas d'activité suspecte (un hacker ayant pris le contrôle d'un équipement public est susceptible de propager son attaque sur le poste nomade et d'investir à terme le système de la collectivité).

TELETRAVAIL

Le télétravail s'effectue selon les règles de la collectivité. Le matériel fourni par l'employeur restant sa propriété, il devra être restitué dès la fin de la période de télétravail.

L'utilisateur est également tenu de prendre soin des équipements qui lui sont confiés. En cas de panne (matériel défectueux…), de problème d'accès (VPN déficient…) ou tout autre incident (vol…), l'utilisateur avisera immédiatement le service informatique.

L'utilisateur en télétravail est soumis aux mêmes obligations générales et dispose des mêmes droits que l'utilisateur qui exécute son travail dans les locaux de l'employeur.

EN CAS DE PANNE

Dans l'intérêt de tous, l'utilisateur signalera au service informatique tout dysfonctionnement affectant la disponibilité des ressources informatiques, ainsi que tout incident semblant porter atteinte à la sécurité du système informatique.

Pour toute demande d'intervention, il est demandé aux utilisateurs de contacter le service informatique par téléphone pour les urgences classées « Très Très Urgentes », bloquantes, ou pour les cas spécifiés par le service informatique. Pour les autres situations, il est demandé d'utiliser l'outil de demande d'intervention en ligne.

Chaque demande sera traitée selon des critères d'urgence (définis par le service informatique), de ressources humaines disponibles et de temps d'intervention.

QUELLES SONT LES RESPONSABILITES DE CHACUN ?

RESPONSABILITES DU SERVICE INFORMATIQUE

L'employeur doit garantir l'intégrité du système informatique de son administration et veiller à ce qu'il ne soit pas fait une utilisation illicite ou fautive d'internet sur le lieu de travail. Le service informatique œuvre pour atteindre cet objectif et recherche une qualité optimale des ressources informatiques et téléphoniques, tant en termes de disponibilité que de sécurité. A cet égard, il est responsable :

- Du paramétrage des logiciels et systèmes pour garantir la sécurité des SI (pare-feu, logiciels de filtrage, anti-virus, anti-spam…) ;
- De la réalisation des sauvegardes, selon les conditions présentées à chacune des catégories de données ;
- De la communication interne pour prévenir de toute interruption ou dégradation de service, ainsi que d'en minimiser la durée ;
- De la mise en œuvre des mesures nécessaires si une utilisation excessive des ressources par un utilisateur nuit au bon fonctionnement général des ressources communes.

Le service informatique opère sans avertissement, à la demande de la hiérarchie ou de l'utilisateur, aux investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'un de ses composants, qui mettent en péril son fonctionnement ou son intégrité.

Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers « logs » sont utilisés en cas de panne, d'intrusion..., c'est-à-dire de manière tout à fait exceptionnelle. Les fichiers « logs » sont utilisés après des défaillances systèmes afin de pouvoir remettre en place le système d'information. Ils recensent toutes les connexions aux différents fichiers ou connexions internet. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'événement.

A des fins de maintenance informatique, le service informatique peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur, et cela tout simplement, pour gagner en temps et en efficacité.

Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus personnels de l'agent.

A des fins d'administration ou de diagnostic, les agents du service informatique peuvent ponctuellement être amenés à manipuler des dossiers enregistrés localement par les utilisateurs. Sauf en cas d'indication très claire permettant d'identifier le caractère personnel du contenu, le service informatique demandera expressément à l'utilisateur d'enlever ces données. Le service informatique n'est pas responsable de la perte des éléments enregistrés sur les supports de stockage locaux (C : ou D :).

Les agents du service informatique s'engagent à respecter scrupuleusement la confidentialité des informations qu'ils manipulent.

Ils sont assujettis au devoir de réserve, comme tous les utilisateurs et sont tenus de préserver la confidentialité des données qu'ils seraient amenés à connaître dans le cadre de leurs fonctions.

Les agents du service informatique peuvent être amenés à contrôler ou piloter l'utilisation des ressources matérielles, logicielles et réseau, ainsi que les ressources téléphoniques. Pour ce faire, ils disposent de logiciels qui exploitent les bases de données numériques pour constituer des tableaux de bords d'analyse des consommations ou utilisations. La diffusion de ces informations est confidentielle et interne. Ces tableaux de bord permettent d'améliorer la sécurité, la vitesse du système d'information.

Ces opérations sont réalisées dans le respect de la loi informatique et libertés, et conformément aux déclarations faites à la CNIL (Commission Nationale de l'Informatique et des Libertés).

Dans le cadre de nos activités, nous nous engageons à respecter les dispositions du Règlement Général sur la Protection des Données (RGPD) en matière de collecte, de traitement et de stockage des données personnelles. Toute information personnelle collectée est traitée de manière confidentielle et sécurisée, dans le respect des droits des utilisateurs. Les données ne sont conservées que pour la durée nécessaire aux finalités pour lesquelles elles ont été collectées et sont protégées par des mesures techniques et organisationnelles adaptées. Chaque individu dispose d'un droit d'accès, de rectification, d'effacement, et de portabilité de ses données, ainsi qu'un droit de limitation ou d'opposition à leur traitement, conformément aux articles 15 à 22 du RGPD.

RESPECT DE LA LEGISLATION

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le Code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par le service informatique.

Cette règle s'applique également pour les logiciels dits « freeware » et « shareware » car la gratuité d'un produit n'induit pas l'autorisation de l'installer : ce dernier peut nuire au fonctionnement du système d'information. Avant toute installation, il est demandé à chaque utilisateur de contacter le service informatique pour validation de la licence, vérification de la sécurité puis installation.

Par ailleurs l'utilisateur ne doit pas installer de logiciels à caractère ludique, notamment par téléchargement, ni contourner les restrictions d'utilisation d'un logiciel. Par conséquent, le service informatique se réserve le droit de désinstaller les logiciels prohibés.

La loi sanctionne certaines fraudes en matière informatique, comme l'indique la loi n°88-19 du 5 janvier 1988 (loi GODFRAIN), complétée par la loi n°2004-575 du 21 juin 2004 :

- Accès frauduleux à un système informatique ;
- Atteintes volontaires au fonctionnement d'un système informatique ;

Tentative d'un de ces délits :

- Association ou entente en vue de les commettre.

Par ailleurs, la législation interdit à tout utilisateur de dupliquer, distribuer ou diffuser des documents (images, sons, vidéos…) soumis au droit de la propriété intellectuelle.

Toute copie de données sur un support externe est soumise à l'accord du responsable hiérarchique direct. Après accord de la hiérarchie, l'utilisateur est responsable de la sauvegarde et de l'intégrité des documents stockés sur des supports amovibles (clé USB, disques externes…).

L'utilisateur s'engage à ne pas tenter d'accéder à des données privées appartenant à un autre utilisateur.

DROIT A LA DECONNEXION

Avec l'utilisation du numérique, l'accès à Office 365, les modes de travail évoluent. Les salariés peuvent être de plus en plus « connectés » en-dehors des heures de bureau, la frontière entre vie professionnelle et personnelle est ténue. C'est donc pour s'adapter à cette réalité et créer les protections nécessaires à la santé des agents qu'un droit à la déconnexion est inscrit dans la présente charte.

COMMUNICATION DE L'INFORMATION

Afin de réduire le stress lié à l'utilisation des outils numériques professionnels, il est également recommandé à tous les agents de :

- S'interroger sur le moment opportun pour envoyer un courriel/SMS ou appeler un collaborateur sur son téléphone professionnel ;
- Ne pas solliciter de réponse immédiate si ce n'est pas nécessaire ;
- Privilégier les envois différés lors de la rédaction d'un courriel en-dehors des horaires de travail, quand cela est possible.

RESPECT DES PERIODES DE SERVICE ET DES CYCLES DE TRAVAIL

L'envoi de messages électroniques est à éviter entre 21h et 7h, le week-end, les jours fériés et pendant les congés. Il n'est pas attendu de réponse aux messages sur ces mêmes créneaux.

Les managers ne peuvent pas contacter leurs collaborateurs entre 21 heures et 7 heures ainsi que pendant les week-ends, congés. Ce principe est modulé en fonction des cycles de travail pour les agents en horaires décalés (ou d'astreintes) et ne s'applique pas en cas de gestion de crise, d'urgence avérée ou de nécessité de service.

Il est rappelé que l'usage de la messagerie électronique ou du téléphone professionnel en-dehors des horaires de travail doit être justifié par la gravité, l'urgence et/ou l'importance du sujet en cause.

DISPOSITIONS DIVERSES

PROCEDURE EN CAS D'ARRIVEE/ DEPART/CHANGEMENT DE POSTE D'UN AGENT

Lors de l'arrivée d'un nouvel utilisateur, le service informatique lui fournit un identifiant et un mot de passe pour accéder à ses ressources ainsi que toutes les informations concernant l'utilisation des réseaux, des outils informatiques et de télécommunications.
Le mot de passe associé à cet identifiant de connexion doit être modifié par l'utilisateur dès sa première connexion.

Lors de son départ, l'utilisateur doit restituer au service informatique les matériels mis à sa disposition. Il doit préalablement effacer ses fichiers et données privés.
Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ.
Avant tout cessation de fonction, il est interdit de supprimer ou de jeter tout élément de la collectivité nécessaire à l'accomplissement des fonctions par des utilisateurs remplaçants. Ce phénomène ne permettrait pas la continuité de service public et ferait obstacle au devoir d'obéissance hiérarchique. Cette désobéissance est passible de sanction disciplinaire.
Les effectifs de la collectivité fluctuent sans cesse (arrivées, départs, mobilités internes), il est nécessaire que les droits et les accès au système d'information soient mis à jour en fonction de ces évolutions. Il est notamment essentiel que l'ensemble des droits affectés à une personne soient révoqués lors de son départ ou en cas de changement de fonction.

Lors du changement de poste dans la collectivité, les habilitations seront revues. En cas d'erreur dans les droits d'accès, l'utilisateur se rapprochera du service informatique.

En cas d'absence momentanée (par exemple, pour une réunion ou une pause déjeuner), il est recommandé de verrouiller l'ordinateur ou de le mettre en veille pour prévenir l'accès non autorisé à vos informations et données. La fonction Windows+L permet de verrouiller l'ordinateur.
Un verrouillage automatique est programmé sur chaque poste de travail après une absence de quelques minutes selon la politique de sécurité de la collectivité. A son retour, l'utilisateur devra saisir son mot de passe de session.
Il est interdit de supprimer/modifier le paramétrage de mise en veille automatique.
En cas d'absence programmée, suivez les procédures spécifiques de la collectivité pour mettre en place une réponse automatique dans votre messagerie électronique, indiquant votre absence et fournissant les coordonnées d'une personne de contact alternative si nécessaire.
Il est interdit d'utiliser la fonction de transfert automatique des mails vers une autre boite mail.
Ne partagez pas votre mot de passe ou vos informations d'identification avec d'autres personnes et ne permettez pas à quiconque d'utiliser votre session informatique.

SANCTIONS

En cas de violation de la charte, l'autorité territoriale pourra suspendre immédiatement les droits d'accès de l'utilisateur aux ressources informatiques, de façon provisoire jusqu'au prononcé de la décision définitive par l'administration.

Cette décision interviendra une fois que l'utilisateur aura été entendu.

Dans l'hypothèse où la violation en cause constituerait une faute passible d'une sanction disciplinaire ou des poursuites pénales, l'intéressé pourra se voir traduit devant la Commission Administrative Paritaire ou le Tribunal (en cas de procédure pénale).

La collectivité se réserve le droit d'engager des poursuites pénales, indépendamment de toute sanction interne mise en œuvre.

PUBLICITE

La charte est diffusée à l'ensemble des utilisateurs dès sa mise en application le 01/01/2025. Elle est systématiquement remise à tout nouvel arrivant pour lecture puis approbation.

FAIT A COSNE-COURS-SUR-LOIRE, le xx/xx/2024
Le Président,
Sylvain COINTAT