CHARTE DE BON USAGE DES RESSOURCES INFORMATIQUES, TELEPHONIQUES ET DES RESEAUX SOCIAUX DES AGENTS DE LA CAPSO ET DU CIAS

1- Objet de la charte

La présente charte a pour objet de définir les règles de bonne utilisation des ressources informatiques des agents de la Communauté d'Agglomération du Pays de Saint-Omer (CAPSO). Il est entendu que le terme « CAPSO » regroupe dans la charte à la fois la CAPSO mais aussi son CIAS.

Les règles de bonne utilisation des ressources numériques relèvent avant tout du bon sens, et visent à assurer à chacun l'utilisation optimale des ressources informatiques dans le respect de la loi et de l'éthique.

La CAPSO met à la disposition de tout utilisateur un système d'information comprenant des équipements informatiques (PC, portables, logiciels, progiciels, matériels d'impression …), des moyens de communication (téléphones fixes et mobiles, messagerie, accès Internet…), ainsi que des informations et données (documents, bases de données, images, vidéos), qui sont nécessaires à l'accomplissement de sa mission. Ce système est partagé par l'ensemble des utilisateurs, mais il demeure la propriété de la CAPSO.

Ces moyens sont accordés à titre individuel sur des critères fondés sur les missions de l'utilisateur et en accord avec son encadrement. Ils doivent être restitués en cas de départ définitif de la collectivité ou de changement de mission, si cette dernière ne nécessite plus leur utilisation.

La fourniture de services numériques est régie par un ensemble de réglementations et de bonnes pratiques. Elles permettent le vivre ensemble numérique et la protection des agents et collectivités.
C'est l'objet de la présente charte.

2- Périmètre/champ d'application

Conformément à la réglementation, la CAPSO est civilement responsable des agissements de ses agents, pour des faits, intentionnels ou non, commis dans le cadre de l'exécution de leurs attributions professionnelles, conformément aux dispositions de l'article 1384 du code civil.

La charte s'applique à tout utilisateur du système d'information déployée par la CAPSO.

Est considérée comme « utilisateur », toute personne, quel que soit son statut (titulaire, contractuel, stagiaire, élu, délégataire, prestataire…) étant amenée à travailler sur le Système d'Information de l'établissement, et autorisée à modifier, consulter et utiliser le système, de façon temporaire ou permanente.

En qualité d'utilisateur du système d'information, chacun s'engage à signer et à appliquer l'ensemble des dispositions de la présente charte exposées ci-dessous.

Ces dispositions ont pour objectif d'informer et de contractualiser les modalités entre l'employeur et les utilisateurs notamment dans le cadre d'une instruction pénale.

Le droit d'accès aux ressources informatiques et de télécommunications est conditionné par l'engagement écrit de l'utilisateur à respecter la charte informatique de la CAPSO. Cet engagement est matérialisé par la signature du formulaire d'acceptation de la charte figurant en annexe.
https://capso365.sharepoint.com/:w:/s/DSI/EVJPIs6p9zxNo-xwuOY_QlkBiiaX4_Mj33cGtENJvGo4YA?e=ohyYYj

3- Règles d'utilisation du système d'information

Le matériel informatique est mis à disposition des utilisateurs pour se connecter sur le réseau. Ce matériel est géré par la Direction du Numérique Intercommunale.

Chaque utilisateur est responsable du bon usage de son équipement. Tout incident doit ainsi être signalé dans les plus brefs délais. Il n'est pas autorisé de déplacer du matériel, de déplacer les connexions réseaux ou téléphoniques vers d'autres prises. Il est interdit d'intervenir dans les bais informatiques hors autorisation et instruction de la Direction du Numérique Intercommunale.
L'intégrité des données partagées par les utilisateurs sur le réseau informatique doit être respectée.
De la même manière, l'usage général des ressources communes doit être fait de façon raisonnée et respectueuse des collègues et de l'activité des services.

L'utilisateur est responsable de l'usage qu'il fait des ressources du système d'information dans l'exercice de sa fonction.

Il doit réserver l'usage de ces ressources au cadre de son activité professionnelle.

Toutefois, un usage privé raisonnable, notamment de la messagerie professionnelle, limité aux nécessités de la vie courante et familiale est toléré en privilégiant le temps de pause méridienne. Cet usage ne doit ni affecter le fonctionnement des systèmes ni perturber l'activité professionnelle. Une consultation ponctuelle et limitée, pour motif personnel, des sites Internet dont le contenu n'est pas contraire à l'ordre public, aux bonnes mœurs et ne mettant pas en cause l'intérêt et la réputation de l'institution est également accordée.

Pour accéder au système d'information, l'utilisateur doit utiliser prioritairement les moyens fournis par la CAPSO. L'usage d'autres outils, notamment du matériel personnel, pour accéder au système d'information doit être soumis préalablement à l'autorisation de la Direction du Numérique. L'utilisation à destination professionnel d'outils personnels est à l'initiative de l'utilisateur et reste de sa responsabilité, la CAPSO ne pourra être tenue responsable en cas de dégradation de ces matériels.

Tenu au devoir de réserve, l'utilisateur ne doit pas divulguer les informations auxquelles il a accès sans autorisation, ou si elles peuvent porter préjudice à la CAPSO ou à une personne physique. L'utilisateur ne doit pas non plus tenter d'accéder aux informations pour lesquelles il n'est pas habilité.

3.1 Respect du cadre législatif et réglementaire

Dans l'utilisation qu'il fait des ressources mises à sa disposition par l'institution, l'utilisateur s'engage à respecter la législation en vigueur (voir chapitre correspondant) relative notamment :

- à l'informatique, aux fichiers, aux libertés,
- à la propriété littéraire, artistique, intellectuelle,
- à la protection de la vie privée,
- au respect de l'ordre public au sens large.

En conséquence, l'utilisateur ne doit se livrer, en aucune circonstance, à l'une quelconque des activités suivantes :

- 1. Charger, stocker, publier, diffuser ou distribuer, au moyen des ressources de la CAPSO, des documents, informations, images, vidéos, etc… :

• à caractère violent, diffamatoire, pornographique ou contraire aux bonnes mœurs, ou susceptibles de porter atteinte au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs,

• portant atteinte aux ressources et missions des collectivités et plus particulièrement à l'intégrité et à la conservation des données du système d'information,

• portant atteinte à l'image et à la réputation de la collectivité.

Il est interdit d'accéder ou de s'inscrire sur des sites Web traitant de ces sujets.
Pour éviter qu'elle ne soit utilisée dans un courrier de masse comportant des pièces jointes illicites, l'inscription sur de tels sites avec l'adresse mail professionnelle de l'utilisateur est proscrite.

Si l'utilisateur est amené à recevoir, à son insu, de tels éléments, il est tenu de les détruire aussitôt, et à prendre contact avec la Direction du Numérique qui l'accompagnera.

L'utilisateur doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents sous forme d'informations, d'images, de vidéos, de fichiers ou autres.

- 2. Utiliser les ressources du système d'information à des fins de harcèlement, menace ou d'injure, et de manière générale à violer les lois en vigueur.
- 3. Charger, stocker ou transmettre des fichiers contenant des éléments protégés par les lois sur la propriété intellectuelle, sauf à posséder les autorisations nécessaires. L'utilisateur s'interdit de solliciter l'envoi par des tiers, en pièces jointes, de tels fichiers.
- 4. Charger, stocker, utiliser ou transmettre des programmes, logiciels, progiciels, etc…, qui sont protégés par les lois sur la propriété intellectuelle, autres que ceux qui sont expressément autorisés par la collectivité. L'utilisateur s'interdit de solliciter l'envoi par des tiers, en pièces jointes, de tels programmes, logiciels, progiciels ou autres.
- 5. Utiliser les matériels, programmes, logiciels, progiciels, mis à sa disposition par la collectivité, en violation des lois sur la propriété intellectuelle, des règles techniques applicables et des prescriptions définies par la collectivité.
- 6. Falsifier la source d'éléments contenus dans un fichier.
- 7. Contrevenir à l'occasion des échanges informatiques aux obligations de discrétion et réserve, de même qu'aux principes de laïcité et de neutralité du service public.

Cas particulier de la collecte de données à caractère personnel :

Dans le cadre de son activité, l'utilisateur peut avoir besoin de traiter des données à caractère personnel (d'administrés, des agents, …). Aussi, préalablement à la constitution d'un fichier comportant des informations nominatives, chaque direction, en collaboration avec la Direction du Numérique, doit s'assurer que les déclarations préalables auprès de la CNIL ont été faites. Dans le cas contraire, la direction concernée est tenue de préparer les documents règlementaires nécessaires à la déclaration ou à l'autorisation des traitements de données nominatives. Toute constitution de fichier comportant des informations nominatives doit être validée par le représentant légal de l'établissement et doit se limiter aux données exclusivement nécessaires à la finalité du traitement. Aucune saisie ne doit comporter de jugement de valeur, de renseignement subjectif ou de valeur qualitative sur les personnes que ce soit dans des fichiers ou les logiciels traitant de données à caractère personnel. Les intéressés ont la possibilité, conformément à la loi « Informatique et libertés » de s'opposer pour des motifs légitimes à ce que les données à caractère personnel fassent l'objet d'un traitement. L'obligation d'information des personnes doit être réalisée, notamment sur les destinataires des données et le lieu où s'exerce le droit d'accès et de rectification.

En conformité avec le RGPD, il est rappelé que la loi du 06 Janvier 1978 prohibe la collecte d'informations nominatives sans déclaration préalable auprès de la CNIL (commission informatique et libertés) des buts de cette collecte et information préalables des personnes concernées. Il est formellement interdit de procéder à la collecte de données nominatives en dehors des déclarations souscrites par la collectivité. Il est rappelé que toute divulgation d'information nominative touchant à la vie privée peut être susceptible de poursuites pénales. Il est interdit de collecter des données par un moyen frauduleux, déloyal ou illicite.

3.2 Les mesures de sécurité à prendre

Tout utilisateur est responsable de l'usage des ressources informatiques auxquelles il a accès.
Il a aussi la charge à son niveau, de contribuer à la sécurité générale du système d'information.
Afin de permettre la mise en œuvre par la Direction du Numérique d'un niveau de sécurité suffisant et de ses procédures associées, l'utilisateur doit respecter au minimum, les prescriptions suivantes :

1. protéger l'accès aux ressources informatiques (matérielles, logicielles, …) par un mot de passe dès lors que c'est possible, y compris pour les téléphones portables,
2. changer de mot de passe régulièrement ou sur demande de la Direction du Numérique,
3. ne jamais confier son identifiant/mot de passe à un tiers y compris le supérieur hiérarchique.
4. ne jamais demander son identifiant/mot de passe à un collègue ou subordonné
5. ne pas laisser en évidence les informations de compte utilisateur, identifiant et mot de passe. Si ces informations sont conservées sous forme écrite, les garder en lieu sûr, mais en aucun cas, elles ne doivent être présentes sur le bureau,
6. ne pas utiliser les identifiants et mot de passe d'une autre personne ce qui est considéré comme de l'usurpation d'identité,
7. ne jamais quitter son poste de travail en laissant accessible une session en cours (mise en veille avec mot de passe après cinq minutes d'inactivité ou verrouillage manuel de la session  +L),
8. protéger spécifiquement les informations confidentielles,
9. ne pas faire de partage réseau de fichiers et répertoires du disque local. Des lecteurs réseaux sont disponibles à cet usage,
10. ne pas laisser à disposition des supports informatiques amovibles (disque dur externe, CD-Rom, clé USB) contenant des données confidentielles, dans un bureau ouvert,
11. sauf exception validée par la Direction du Numérique, l'utilisation des supports amovibles de type clé USB doit être limitée au transfert de données entre matériels qui ne sont pas connectés au même réseau. Le support amovible, doit être vidé de tout contenu après utilisation pour éviter la propagation de données sensibles en cas de perte ou de vol,
12. le stockage de documents privés (photos, bureautique) est toléré sur les disques des postes de travail et en aucun cas sur les espaces partagés. L'utilisateur est informé que :
    • tout document stocké sur une ressource mise à disposition par la collectivité est réputé professionnel SAUF s'il est stocké dans un répertoire portant la mention « **Personnel et Confidentiel** »,
    • le fonctionnement du poste de travail ne doit pas être altéré par le stockage de documents privés,
    • les documents privés stockés doivent respecter le cadre légal et réglementaire,
    • les disques locaux des postes de travail ne sont pas sauvegardés. Par conséquent, les documents privés stockés sur ces disques peuvent être définitivement perdus en cas de problème technique sans que la responsabilité de la collectivité puisse être engagée,
    • les postes de travail pouvant être partagés entre plusieurs utilisateurs, seuls les documents enregistrés dans le répertoire « Mes documents » seront accessibles par l'utilisateur.
13. Le recours aux sessions génériques n'est permis que pour les bornes d'accès grand public faisant l'objet de dispositions particulières de sécurité.

La Direction du Numérique via ses administrateurs réseaux et systèmes est seule autorisée à accéder et à extraire les données utilisateurs sur instruction du représentant légal de l'établissement ou sur requête des autorités judiciaires.

3.3 Matériels, progiciels, logiciels, données

L'utilisateur s'interdit de modifier les équipements mis à sa disposition, notamment par l'ajout de logiciels sur les postes de travail. Toute tentative de désinstallation de logiciels standards est proscrite, celle-ci pouvant provoquer un dysfonctionnement du poste de travail. À des fins de précaution, certaines configurations de postes de travail peuvent être verrouillées par la Direction du Numérique. Le poste de travail de chaque utilisateur est protégé par un logiciel antivirus.

Cependant, l'utilisation des applications communicantes (Internet, messagerie) et des supports de stockage (disque dur externe, CD-Rom, clé USB) peut, malgré les précautions prises, provoquer la transmission et l'installation sur le poste de travail de l'utilisateur, à l'insu de ce dernier, de programmes ou fichiers, qui altèrent ou pillent les données et logiciels qu'il contient.
En cas d'anomalie, l'utilisateur doit stopper toute transaction, quitter les applications en cours, arrêter son poste de travail, et prévenir immédiatement la Direction du Numérique (*dirnum@ca-pso.fr*).

Afin de préserver le bon fonctionnement et la cohérence du Système d'Information, tout choix et/ou commande de logiciels ou progiciels et développements de logiciels spécifiques, données amenées à être installées dans le parc informatique ne pourront se faire qu'avec l'accord préalable de la Direction du Numérique.
Les utilisateurs connectés au réseau disposent de plusieurs moyens d'impression, suivant leur localisation géographique. L'implantation de ces matériels est définie par la Direction du Numérique en relation avec les directions concernées.

Toute installation ou déménagement de poste de travail doit se faire avec l'accord préalable des services techniques compétents, notamment en ce qui concerne les branchements électriques et informatiques. Pour la bonne organisation et préparation, l'agent formalisera sa demande par le biais des outils disponibles sur Intranet.

3.4 Respect du matériel

Il convient de préserver le matériel appartenant aux collectivités.

1. Eteindre son poste par arrêt logiciel pour terminer proprement ses sessions (hors cas de blocage technique).
2. Eteindre son poste par arrêt logiciel la nuit et le week-end, et plus généralement durant toute absence prolongée (sauf demande particulière de la Direction du Numérique).
3. En cas de perte ou de vol, avertir immédiatement votre service et la Direction du Numérique.
4. Eviter la consommation de nourriture, boissons, et de manière générale toute utilisation de substance pouvant endommager le matériel.
5. Prendre soin des appareils mobiles (téléphone, smartphone, ordinateur portable, …) qui sont particulièrement fragiles et convoités.

En cas de dégradation ou de vol de matériel et si un non-respect des consignes de sécurité est avéré, la responsabilité de l'agent pourra être engagée pour les frais occasionnés pour la réparation ou le remplacement du matériel endommagé.

3.5 Recommandations spécifiques aux utilisateurs en situation de mobilité

Afin de préserver la confidentialité des données stockées sur les disques locaux et d'assurer la sécurité des matériels, il est demandé de respecter les consignes suivantes :

1. Eviter toute imprudence ou mauvaise utilisation qui pourrait engager votre responsabilité personnelle,
2. Ne pas exposer le matériel à des conditions climatiques agressives (humidité, soleil etc…),
3. Ne pas laisser le matériel sans surveillance (dans les transports en commun par exemple),
4. Ne pas le prêter,
5. Tout ordinateur portable mis à disposition doit être rendu exclusivement à la Direction du Numérique à la fin de son utilisation. Il est rappelé à l'utilisateur qu'il a la responsabilité du matériel qui lui est confié jusqu'au retour à la Direction du Numérique. En particulier pour les réunions en fin de journée, le matériel ne doit, ni être laissé en salle de réunion, ni déposé à l'accueil,
6. Supprimer tous les fichiers temporaires du portable,
7. Dès que le matériel est connecté au système d'information de la collectivité (*attention à la bonne utilisation du VPN et partage de connexion*), enregistrer les documents modifiés sur les espaces de stockage sécurisés,
8. Supprimer tous les documents non indispensables pour éviter les risques de divulgation d'informations stratégiques en cas de perte ou de vol du matériel.

3.6 Organisation des espaces de stockage des documents bureautiques

La Direction du Numérique met à disposition des utilisateurs connectés au réseau principal, plusieurs espaces de stockage réseau organisés selon la destination des fichiers.

• *Direction/Service* : cet espace est accessible aux agents de la structure, c'est l'espace dans lequel doivent être stockés les documents professionnels susceptibles d'être partagés au sein du service,

• *Commun* : cet espace est accessible à tout le monde, c'est un espace qui permet de partager des documents entre services. Ce n'est pas un espace de partage ou de travail permanent. Cet espace ne doit pas comporter de documents confidentiels qui ne soient pas protégés par des mots de passe. A terme suppression des données chaque semaine.

Les utilisateurs doivent respecter l'organisation mise en place pour le stockage des données dans l'espace de stockage bureautique de chaque service et dont les principes sont les suivants :

- Organiser le volume bureautique de façon générique (éviter les répertoires individuels) de manière à faciliter les recherches. Chaque service doit créer sa propre arborescence en fonction de ses missions.

- Supprimer les fichiers obsolètes ou sans intérêts de manière à récupérer de l'espace disque sur le serveur bureautique.

Dans la mesure du possible, aucun document ne doit être stocké localement sur le disque dur du poste de travail : ces données ne sont pas sauvegardées. En cas de vol aucune confidentialité ne peut être garantie, de plus, ce stockage a pour conséquence une altération des performances du poste de travail. Le disque dur du poste de travail de l'utilisateur et les espaces de stockage du réseau ne doivent pas contenir de programmes, logiciels, documents, fichiers, informations ou données, à caractère violent, pornographique, contraire aux bonnes mœurs, ou susceptibles de porter atteinte au respect de la personne humaine et de sa dignité, ainsi que tout autre fichier prohibé par la loi.

L'accès aux données personnelles et confidentielles ne pourra être réalisé qu'en cas de risque ou évènement particulier, et en présence de l'utilisateur, à sa demande ou après l'avoir convoqué à cette fin.

Lors de son départ, un utilisateur devra supprimer les données d'ordre personnel. Les données d'ordre professionnel devront impérativement être distribuées aux agents du service reprenant le dossier ou mises à disposition du remplaçant ou encore de la personne en charge de l'archivage numérique.
Toutes les informations relatives à l'utilisateur seront supprimées par les administrateurs systèmes et réseaux de la Direction du Numérique après son départ.

Afin de garantir la pérennité, la sécurité et l'accessibilité des données, il est formellement proscrit d'échanger et de stocker ces données en dehors du système d'information de la CAPSO ("cloud" internet, dropbox, stockage externalisés, webtransfert…)
L'utilisation d'espaces de travail collaboratifs mis à disposition par des partenaires est soumise à autorisation de la Direction du Numérique. Dans ce cas, l'utilisateur reste seul responsable des informations mises à disposition sur l'espace de travail.

3.7 Utilisation de la messagerie

L'utilisateur est responsable du contenu des messages qu'il envoie et qu'il transfert volontairement après réception, ainsi que de leur destination.

L'utilisateur ne doit pas perturber le fonctionnement général du système d'information par un usage abusif de la messagerie (nombre de messages conservés trop important, distribution multiple, pièces jointes volumineuses, etc...).

La Direction du Numérique a mis en place des dispositifs de contrôle anti-virus ; pour autant, l'utilisateur doit rester vigilant quant au contenu des données des messages et en provenance d'Internet.

En particulier, il est fortement conseillé de détruire les messages d'origine inconnue sans les ouvrir.

L'utilisation des outils de messagerie électronique est réservée à un usage professionnel. Un usage personnel est toutefois admis de manière ponctuelle pour répondre aux besoins de la vie quotidienne. Tout message émis ou reçu via la messagerie électronique est considéré comme professionnel SAUF si l'objet contient la mention « Message personnel ».

L'utilisateur ne doit jamais écrire dans un message électronique ce qu'il s'interdirait d'exprimer oralement ou par un autre moyen (courrier, télécopie).
De même que partout ailleurs, la courtoisie constitue une règle de base dans tous les échanges électroniques (Cf. Charte de bon usage).

L'utilisateur doit être conscient qu'un message électronique peut :

- être stocké, réutilisé, exploité à des fins auxquelles l'utilisateur n'aurait pas pensé en le rédigeant,
- constituer une preuve ou un commencement de preuve par écrit.

Par conséquent, une grande prudence est à observer dans l'utilisation du courrier électronique à destination des tiers.
L'utilisateur doit utiliser avec discernement les listes de diffusion personnelles ou collectives. Il doit éviter l'envoi de copies à un nombre injustifié de destinataires. Il ne doit pas diffuser de l'information non souhaitée par les destinataires (SPAM).
L'envoi des messages en masse (nombreux destinataires) en dehors du cadre professionnel est interdit. Il n'est pas permis de s'inscrire à des listes de diffusion extérieures au cadre professionnel avec son adresse de messagerie professionnelle. En outre, l'adresse de messagerie professionnelle ne peut en aucune manière être l'adresse officielle d'une structure externe aux collectivités (association par exemple). Il est par ailleurs déconseillé d'afficher à l'externe pour une mission de service public une adresse nominative (ex : *contact@ca-pso.fr et non jc.dusse@____)*

3.8 Utilisation d'Internet

Vous êtes responsable de l'usage que vous faites d'Internet, et plus particulièrement du choix des sites visités.

L'utilisateur doit veiller à ne pas perturber le fonctionnement général du système d'information par un usage abusif des accès à Internet (connexion permanente, utilisation de logiciels de navigation automatique, rapatriement et stockage massif de fichiers à usage personnel, …).
Il est rappelé que la plupart des sites Internet visités gardent une trace de chaque passage. L'attention de l'utilisateur est attirée sur ce point et il lui est demandé de prendre toutes les précautions à cet égard. L'utilisateur engage sa responsabilité personnelle en ce qui concerne les sites visités et le contenu de ceux-ci.

L'attention des utilisateurs est appelée sur le fait que tout téléchargement peut comporter certains risques juridiques (voir chapitre correspondant) et techniques notamment l'introduction de virus malgré les dispositions prises à travers les dispositifs de sécurité mis en œuvre par la Direction du Numérique.

Pour des raisons techniques, l'historique des connexions Internet des utilisateurs est enregistré. Ces informations sont conservées pendant 6 mois et sont susceptibles d'être communiquées, sur décision judiciaire, aux services de police, conformément aux préconisations de l'ANSSI (Agence nationale de la Sécurité des Systèmes d'Information).

A des fins de statistiques, de qualité de service et de sécurité, le trafic Internet pourra faire l'objet d'une supervision ou de vérifications par la CAPSO, dans les limites prévues par la loi.

3.9 Utilisation des logiciels ou progiciels métiers

Les collectivités mettent à la disposition de l'utilisateur des ressources (Intranet, Extranets, logiciels, progiciels …) pour exercer son activité professionnelle conformément aux règles juridiques et techniques applicables et aux prescriptions définies.

Les habilitations applicatives sont déterminées par la direction gestionnaire de l'outil concerné. Elles sont liées aux fonctions occupées et peuvent de ce fait évoluer dans le temps.

Les informations de connexion sont strictement personnelles et ne peuvent en aucun cas être transférées, même temporairement à un tiers.

La Direction du Numérique déploie progressivement l'authentification unique en fonction des capacités techniques des éditeurs pour simplifier et sécuriser la gestion des mots de passe.

3.10 Utilisation de la téléphonie fixe

Le téléphone fixe est un outil mis à la disposition de l'utilisateur à titre professionnel. Une tolérance pour des usages personnels occasionnels est acceptée.

L'agent peut disposer d'un poste téléphonique avec un numéro nominatif identifié. L'utilisateur bénéficie du droit au secret des communications téléphoniques qui s'applique à l'ensemble des messages émis et reçus par le biais de son poste téléphonique

3.11 Utilisation de la téléphonie mobile

Dans le cadre de ses missions, l'utilisateur peut se voir attribuer un téléphone portable de façon temporaire ou durable. Pour ces équipements spécifiques, il est proposé deux modes de fonctionnement.

3.11.1 Téléphone de service

Le téléphone est partagé par plusieurs utilisateurs (astreintes, déplacements, …). Une tolérance pour des usages personnels et occasionnels est acceptée de manière très ponctuelle. L'utilisateur est responsable du matériel, il doit notamment :
• Informer la Direction du Numérique de toute anomalie sur le matériel
• Rendre le matériel en bon état de fonctionnement pour l'utilisateur suivant (appareil propre, batterie chargée, accessoires présents, …)
• Ne pas stocker d'informations personnelles (photos, contacts, …) sur les téléphones de service
• Ne pas installer d'application sur les téléphones de service sans accord préalable de la Direction du Numérique
• Ne pas transférer les appels vers un téléphone portable n'appartenant pas à la collectivité (le transfert d'appel vers un téléphone fixe est autorisé)

3.11.2 Téléphone attribué

Le téléphone est attribué nominativement à un utilisateur. La collectivité et l'utilisateur souscrivent une option de type « Pro/Perso » auprès de l'opérateur de téléphonie titulaire du marché.

Dans ce cas, les collectivités prennent en charge la fourniture du terminal, l'abonnement téléphonique et un volume de communication correspondant à l'activité professionnelle. L'utilisateur est responsable du matériel qui lui est attribué et de l'utilisation qui en est faite (notamment la consultation de sites internet sur les smartphones).

L'utilisateur doit notamment :

• Informer la Direction du Numérique de toute anomalie sur le matériel

• Informer la Direction du Numérique de toute modification d'utilisation professionnelle pouvant entraîner des surcoûts (déplacements professionnels à l'étranger, envoi de SMS en masse, …). Dans l'idéal, l'information doit être donnée à la Direction du Numérique un mois avant que la modification de situation soit effective (pour prise en compte dans la facturation).

• Pour les terminaux de type Smartphone, protéger le verrouillage de l'écran par un code ou un mot de passe,

• Supprimer les informations personnelles (mails, SMS, photos, contacts, …) avant de restituer son téléphone,

De son côté, la collectivité :

• Peut souscrire des options auprès de l'opérateur, les coûts de ces options étant à la charge de la collectivité

• Moduler le volume de communication pris en charge par la collectivité

• N'ont pas accès au détail des communications de l'utilisateur en vertu du droit à la protection de la vie privée

3.11.3 Usage des téléphones personnels

L'usage des téléphones personnels dans le milieu professionnel ne doit pas aller à l'encontre du travail de l'agent et donc de l'intérêt de la collectivité. Les smartphones sont de plus en plus banalisés. Il serait donc difficile d'interdire leur usage dans le milieu professionnel. Toutefois, leur utilisation doit rester limitée, occasionnelle et discrète (appels et sms). Il est également rappelé qu'en cas de détérioration, perte, vol,… sur le temps de travail, la collectivité ne pourrait être tenue responsable.

Les règles rappelant les bons usages en ce qui concerne l'utilisation des outils mail, téléphone, … sont reprises en annexe. Elles visent à permettre une meilleure utilisation de ces outils.

4- L'usage des réseaux sociaux

L'obligation de neutralité et le devoir de réserve s'imposent aux agents publics, y compris dans leur vie privée lorsqu'ils participent à des forums, des listes de discussion ou des blogs. Ils ne doivent pas, dans leurs propos, critiquer leur administration employeur (élus, supérieur hiérarchique, collègues,…) ou, de manière générale, les pouvoirs publics.

Ainsi, des propos qui traduisent un manque de respect du fonctionnaire à l'égard de ses collègues de travail et de sa collectivité et conduisent à discréditer l'autorité administrative et les services sont constitutifs d'un manquement à l'obligation de réserve et passibles de poursuites disciplinaires.

L'administration peut ainsi sanctionner un agent en raison de propos tenus à partir d'un réseau social (Facebook, twitter,…). Des poursuites pénales peuvent également être engagées selon la gravité des faits reprochés.

A titre d'exemple, il est rappelé que les informations publiées sur une page « publique » d'un réseau social, accessible à tout internaute, ne peuvent être considérées comme privées. Les informations deviennent également publiques lorsqu'elles sont rendues accessibles, comme le permet Facebook, aux « amis des amis » du titulaire du profil.

Par ailleurs, il ne suffit pas de limiter ses publications sur Facebook à ses « amis » pour en préserver, dans tous les cas, le caractère privatif. En fonction du contexte, des informations pourtant initialement limitées aux « amis » pourraient en effet perdre leur caractère privatif si une publicité importante leur est donnée, notamment en raison du nombre d' « amis » ayant accès aux informations ou du fait que certains fassent partie du personnel, voire des clients, de l'entreprise ou de l'administration concernée.

5- Droits et devoirs des utilisateurs

Afin d'assurer la sécurité du système d'information ainsi que le respect des règles définies ci-dessus et de disposer de données statistiques, la collectivité a mis en place les outils de monitoring et de contrôle suivants :
• Identification et filtrage des références des émetteurs et des destinataires des messages ou fichiers,
• Contrôle et filtrage anti-virus,
• Contrôle et filtrage du type des fichiers joints émis et réceptionnés,
• Contrôle de la taille des fichiers émis, réceptionnés et stockés et filtrage des fichiers,
• Filtrage des sites accessibles,
• Liste des sites Internet ayant été visités par l'utilisateur avec horodatage de la connexion

Les contrôles pourront être effectués de manière permanente ou ponctuelle en fonction des besoins, des risques ou des incidents détectés. Les données collectées seront traitées par le directeur du Numérique en fonction de la nature des incidents détectés. Elles seront conservées pour une durée de six mois, conformément aux exigences de la CNIL.

Ces moyens de contrôle ont été mis en œuvre en application de la réglementation en vigueur.

Conformément aux articles 39 et 40 de la Loi Informatique et Liberté du 6 janvier 1978, l'utilisateur dispose d'un droit d'accès et de modification des informations le concernant et issues de ces contrôles. L'exercice de ce droit est applicable auprès de la Direction des Ressources Humaines.

En cas de non-respect des règles définies dans le présent document, l'utilisateur encourt la suspension ou la suppression de tout ou partie des moyens mis à sa disposition, sans préjuger des éventuelles suites disciplinaires.
En cas de manquement revêtant un caractère pénal, la responsabilité de l'utilisateur pourra être recherchée devant les tribunaux, à l'initiative de l'employeur ou de tierces victimes.

Les règles définies dans le présent document correspondent aux règles essentielles que l'utilisateur s'engage à respecter. L'attention de l'utilisateur est toutefois attirée sur le caractère non limitatif des présentes règles, qui s'appliquent sans préjudice du respect des autres lois, textes ou usages en vigueur régissant ses activités sur le système d'information.

6- Références légales et législatives

- Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiées et ses textes d'application.

- Code pénal : dispositions relatives aux atteintes aux droits de la personnalité résultant des fichiers ou des traitements informatiques (art. 226-15 à 24), dispositions relatives aux atteintes aux systèmes de traitement automatisés de données (art. 323-1à 323-7) et dispositions relatives à la responsabilité pénale de la personne morale (art 323-6 dans conditions prévues art 121-2).

- Loi du 3 juillet 1985 sur la protection des logiciels par le droit d'auteur et loi du 1er juillet 1992 relative au Code de la Propriété Intellectuelle (CPI).

- Loi (646) du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications. • Code du Travail notamment en ses dispositions suivantes : (principe de proportionnalité (L1121-1), information-consultation préalable du Comité d'Entreprise sur la mise en oeuvre de moyens de contrôle des salariés (L 1121-9) obligation d'informer le salarié ou candidat à l'emploi sur dispositif informatisé le concernant (L 1222-4) information-consultation du Comité d'entreprise pour l'introduction de nouvelle technologie modifiant les conditions de travail (L 2323-32).

- Loi 96-659 du 26 juillet 1996 : réglementation des télécommunications et décrets d'application sur la cryptologie.

- Loi pour la confiance dans l'économie numérique : loi 2004 – 575 du 21 juin 2004 - Chapitre 2 article 6.

- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (RGPD-DPO)