Comité Social Territorial placé auprès du Centre de Gestion

CHARTE INFORMATIQUE

SOMMAIRE

INTRODUCTION

Le contexte et les enjeux

Les différents outils technologiques utilisés offrent au personnel une grande ouverture vers l'extérieur. Cette ouverture peut apporter des améliorations de 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 importantes. En effet, ils augmentent les risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité du Centre De Gestion, d'atteinte à l'intégrité et à la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vols de données).
De plus, mal utilisés, les outils informatiques peuvent aussi être une source de perte de productivité et de coûts additionnels.

L'objectif

La présente charte informatique est un code de déontologie formalisant les règles légales et de sécurité relatives à l'utilisation de tout système d'information et de communication au sein de la collectivité.

Le manquement à la présente charte pourra entraîner le retrait du droit d'utilisation d'un outil, d'une application ou d'un matériel informatique/téléphonique et/ou des mesures d'ordre disciplinaire et/ou des sanctions pénales.

Le champ d'application

La présente charte s'applique à **l'ensemble du personnel tous statuts confondus, ainsi qu'au personnel temporaire et aux élus et/ou aux organisations syndicales installées dans les locaux, en ce qui les concernent.**
Elle s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques de la collectivité. Tout contrat avec un prestataire extérieur devra faire référence et comporter comme annexe la présente charte.

Dés l'entrée en vigueur de la présente charte, chaque individu concerné, devra en prendre connaissance.

I - LES REGLES GENERALES D'UTILISATION

Les utilisateurs sont supposés adopter un comportement responsable s'interdisant par exemple toute tentative d'accès à des données ou à des sites qui leurs seraient interdits.

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient entraîner des conséquences néfastes sur le fonctionnement du réseau. Il doit en permanence garder à l'esprit que c'est sous le nom de l'établissement qu'il se présente sur Internet et doit se porter garant de l'image de l'institution.

Les devoirs des agents publics s'appliquent dans l'utilisation des outils numériques et informatiques. En ce sens, les agents devront observer les règles de neutralité, de confidentialité et de réserve qui incombe à tout agents publics, cela implique notamment que, chacun est responsable des messages envoyés ou reçus. Les agents doivent utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues, des règles élémentaires de courtoisie et de bienséance.

A - Les droits et les devoirs des utilisateurs

Un accès aux ressources réglementé

Le personnel du CDG66 dispose d'un droit d'accès au système d'information.
Ce droit d'accès est :

- Strictement personnel.
- Incessible.

Une utilisation professionnelle des ressources

Les ressources informatiques mises à disposition constituent un outil de travail nécessaire. Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l'utilisation des ressources et notamment :

- Respecter l'intégrité et la confidentialité des données.
- Ne pas perturber la disponibilité du système d'information.
- Ne pas stocker ou transmettre d'informations portant atteinte à la dignité humaine.
- Ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée (loi « informatique et liberté » du 06/01/1978).
- Respecter le droit de propriété intellectuelle : non reproduction et/ou non-diffusion de données soumises à un droit de copie non-détenu, interdiction de copie de logiciel sans licence d'utilisation.
- Ne pas porter atteinte à la sécurité du système d'information par l'utilisation de "ressources extérieures" matérielles ou logicielles.
- Respecter les contraintes liées à la maintenance du système d'information.
- Signaler les messages suspects ou les tentatives d'intrusion du système informatique.

Ces obligations s'appliquent également aux représentants du personnel dans l'exercice de leur activité syndicale au sein des locaux du CDG66 lorsqu'ils utilisent les ordinateurs mis à disposition par l'établissement.

B - Les droits et les devoirs de l'établissement

Le CDG66 s'engage à respecter les règles légales de protection des données à caractère personnel.
Conformément aux exigences du RGPD et de la loi informatique et libertés, le CDG met en place les mesures techniques et organisationnelles afin de garantir la sécurité des données et respecter les principes de confidentialité, intégrité et disponibilité des données.
De plus, le CDG66 respecte les données de chaque agent et s'engage à ne collecter que les données nécessaires à la finalité poursuivie et garantit les droits les concernant (d'accès, information, rectification, opposition, et effacement).
Tous les agents peuvent consulter leurs droits sur www.cnil.fr.

- ***L'INFORMATION INDIVIDUELLE*** *:*

L'employeur peut satisfaire à cette obligation par la diffusion de tous documents précisant les règles d'usage de son système d'information ainsi qu'à leur application (charte informatique, règlement intérieur, note de service...).
Le Comité Social Territorial compétent doit être consulté sur le sujet.

- ***LA DISPONIBILITE ET L'INTEGRITE DU SYSTEME INFORMATIQUE*** *:*

L'établissement s'engage à :

- Mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission du personnel du CDG66.
- Mettre en place des programmes de formations adaptés et nécessaires aux utilisateurs pour une bonne utilisation des outils.
- Informer les utilisateurs des diverses contraintes d'exploitation (interruption de service, maintenance, modification de ressources, …) du système d'information susceptibles d'occasionner une perturbation.
- Effectuer les mises à jour nécessaires des matériels et des logiciels composant le système d'information afin de maintenir le niveau de sécurité en vigueur dans le respect des règles d'achat et des budgets alloués.
- Respecter la confidentialité des "données utilisateurs" auxquelles il pourrait être amené à accéder pour diagnostiquer ou corriger un problème spécifique.

C – L'analyse et le contrôle

Le responsable des systèmes d'information est tenu au respect des règles déontologiques et au secret professionnel. A ce titre, aucune exploitation à d'autres fins que celles liées à la sécurité des applications, des informations dont il peut avoir connaissance dans l'exercice de ses fonctions ne saurait être opérée d'initiative ou sur ordre de sa hiérarchique. Il ne saurait non plus être contraint de le faire, sauf dispositions législatives en ce sens.

Le responsable Informatique est aussi chargé de veiller au respect des règles déontologiques et de bons usages énoncés dans cette présente charte. A ce titre, il est amené à faire des observations et à intervenir auprès des utilisateurs ou de leurs responsables hiérarchiques s'il constate des abus ou des comportements qui perturbent le système.

D - Les sanctions

La Loi, les textes réglementaires (cf. pages 11 et 12) et la présente charte définissent les droits et obligations des personnes utilisant les ressources informatiques.
Tout utilisateur du système d'information de l'établissement n'ayant pas respecté la loi pourra être poursuivi pénalement (cf. pages 11 et 12)
En outre, tout utilisateur ne respectant pas les règles définies dans cette charte est passible de mesures qui peuvent être internes à l'établissement et/ou de sanctions disciplinaires proportionnelles à la gravité des manquements constatés par l'Autorité territoriale.

E - Les évolutions

Avant son entrée en vigueur, la charte est soumise à l'avis du Comité Social Territorial. Dans l'hypothèse où la charte devait être complétée ou modifiée par l'Autorité territoriale, l'avis du Comité Social Territorial serait à nouveau sollicité.

II - LES POSTES INFORMATIQUES

- Un ensemble "matériels - système d'exploitation - logiciels" est mis à disposition de chaque utilisateur :
  - Matériel : unité centrale, écran, clavier, souris…,
  - Système d'exploitation : Windows …,
  - Logiciel : pack bureautique, logiciels de communication, logiciels de gestion, applications spécifiques.

Le matériel informatique est fragile, il faut en prendre soin et redoubler d'attention pour les écrans plats.

- Toute installation logicielle est à la charge de la personne compétente et désignée par l'Autorité territoriale.
- En cas d'absence momentanée, l'utilisateur doit verrouiller son PC (Ex. : maintenir enfoncées les touches 'Ctrl+Alt+Suppr' et cliquer sur 'Verrouiller l'ordinateur').
- En cas d'absence prolongée, l'utilisateur doit quitter les applications et verrouiller son PC.
- A la fin de sa journée de travail, l'utilisateur doit quitter les applications, arrêter le système par arrêt logiciel, éteindre l'écran.
- Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tiers et régulièrement modifiés (deux fois par an).
- La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde quotidienne des informations.
- L'utilisateur doit signaler tout dysfonctionnement ou anomalie au service ou référent informatique selon la procédure définie par la collectivité.
- L'utilisateur doit procéder régulièrement à l'élimination des fichiers non-utilisés et à l'archivage dans le but de préserver la capacité de mémoire.
- Les supports amovibles (CD, clé USB, etc.) provenant de l'extérieur doivent être soumis à un contrôle antivirus préalable.

Tout document ou mail non spécifiquement déterminé comme privé pourra faire l'objet d'un accès conformément au point C de la présente charte.

Le matériel informatique mis à disposition des organisations syndicales est fourni selon la représentativité aux élections professionnelles du Comité Social Territorial placé auprès du CDG 66, celui-ci concerne :

- Des ordinateurs portables pour la durée du mandat syndical.
- Ce matériel est placé sous l'entière responsabilité des organisations syndicales qui détiennent le bon usage et/ou l'affectation de ce matériel à leurs représentants.
- Le CDG66 décline toute responsabilité en cas de vol, casse, perte et/ou mauvais usage de fonctionnement en raison de téléchargement non conforme aux prescriptions de la présente charte. Le matériel ne serait pas remplacé pour ces motifs.

III – LA MESSAGERIE pour le personnel du CDG66

- L'utilisation de la messagerie est réservée à des fins professionnelles. Néanmoins il est toléré en dehors des heures de travail un usage modéré de celle-ci pour des besoins personnels et ponctuels.
  La lecture des courriels personnels reçus durant les heures de travail est tolérée si celle-ci reste occasionnelle.

- L'utilisateur veillera à ne pas ouvrir les courriels dont le sujet paraîtrait suspect.

- Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'Autorité Territoriale ou le référent informatique (même en l'absence de l'utilisateur). Les courriers à caractère privé et personnel doivent expressément porter la mention « personnel » dans leur objet. Ces derniers ne pourront alors être ouverts par l'Autorité territoriale ou le référent informatique, que pour des raisons exceptionnelles de sauvegarde de la sécurité ou de préservation des risques de manquement de droit des tiers ou à la Loi.

- L'utilisateur s'engage à ne pas envoyer en dehors des services de la collectivité des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel et autorisé par son supérieur hiérarchique.

- L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminées.

- L'utilisateur signera tout courriel professionnel.

- L'utilisateur doit vérifier la liste des destinataires et respecter les circuits de l'organisation ou la voie hiérarchique le cas échéant.

- L'utilisateur doit vérifier le contenu et l'historique des messages transférés.

- L'utilisateur doit éviter de surcharger le réseau d'informations inutiles. Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.

- En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant la date de retour prévue. Un agent du service doit pouvoir gérer les messages pendant son absence.

- La signature électronique (loi n° 2000-230 du 13 mars 2000) est présumée fiable jusqu'à preuve du contraire. Son utilisation est limitée aux personnes autorisées et doit respecter la procédure définie par la collectivité.

IV – LE TELETRAVAIL

Conformément à la délibération fixant la mise en œuvre du télétravail au sein du CDG 66, le télétravailleur s'engage à respecter les règles de sécurité en matière informatique.

- L'agent en situation de télétravail s'engage à utiliser le matériel informatique qui lui est confié dans le respect des règles en vigueur en matière de sécurité des systèmes d'information.

- Le télétravailleur doit se conformer à l'ensemble des règles en vigueur au sein de son service en matière de sécurité des systèmes d'information et en particulier aux règles relatives à la protection et à la confidentialité des données et des dossiers en les rendant inaccessibles aux tiers. Par ailleurs, le télétravailleur s'engage à respecter la confidentialité des informations obtenues ou recueillies dans le cadre de son travail et à ne pas les utiliser à des fins personnelles.

- Conformément au RGPD, les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions de l'établissement.

- L'agent en télétravail ne rassemble ni ne diffuse de téléchargement illicite via l'internet à l'aide des outils informatiques fournis par l'employeur. Il s'engage à réserver l'usage des outils informatiques mis à disposition par l'administration à un usage strictement professionnel.

- Le télétravailleur s'engage à être le seul à utiliser le matériel mis à disposition par le CDG 66 et à restituer le matériel à l'issue de la durée d'autorisation d'exercice des fonctions en télétravail.

- Le télétravailleur s'engage à respecter la charte informatique rappelant notamment le maintien du bon fonctionnement et de la bonne sécurité des outils informatiques. (Voir II – Les postes informatiques)

- Le télétravailleur doit disposer à minima de l'ordinateur fourni par le CDG, d'une connexion internet fiable et d'un VPN (Virtual Private Network).

V – LES SITES INTERNET

- Conformément aux règles générales (Voir I), l'utilisation d'Internet est réservée à des fins professionnelles et/ou syndicales.

- Néanmoins, il est toléré pour un usage modéré d'accéder à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.

- L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine (pédopornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminées).

- Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.

- Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

- Tout abonnement payant à un site web ou à un service via Internet doit faire l'objet d'une autorisation préalable de l'Autorité territoriale.

- Pour éviter les abus, l'Autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites les plus visités.

- L'utilisation de forums de discussion est autorisée pour un usage professionnel sous réserve du respect des devoirs des agents publics (réserve, neutralité, etc.).

VI – LES RESEAUX SOCIAUX

- L'utilisation des réseaux sociaux est réservée à des fins professionnelles. Néanmoins il est toléré pour un usage modéré de celui-ci pour des besoins personnels et ponctuels.

  La consultation des comptes personnels durant les heures de travail est tolérée si celle-ci reste occasionnelle.
- L'utilisation doit être appropriée et doit respecter les devoirs des agents publics.
- Le Directeur Général des Services détermine les agents habilités à communiquer sur les réseaux sociaux en nom et pour le compte de l'Institution.
- La distinction entre l'utilisation professionnelle et l'utilisation personnelle est recommandée (création de deux profils)

VII – LE TELEPHONE

Cette présente partie a pour objectif d'établir les règles d'utilisation du téléphone.

Règles d'utilisation

- L'utilisation des téléphones fixes et portables est réservée à des fins professionnelles. Néanmoins, un usage ponctuel du téléphone pour des communications personnelles locales est toléré à condition que cela n'entrave pas l'activité professionnelle et ne représente pas un coût déraisonnable pour le CDG. Peut-être définit comme déraisonnable une communication téléphonique utilisant un numéro spécial à des fins personnelles et dont la facture dépasserait un seuil de 15 euros. Dans cette hypothèse le CDG se réserve le droit de réclamer la somme à l'agent concerné.

- L'utilisation des téléphones portables personnels doit rester, limitée, occasionnelle et discrète (appels et sms).

- L'Autorité Territoriale peut procéder au contrôle de l'ensemble des communications faites par les outils fournis par le Centre de Gestion (téléphones, ordinateurs, logiciels).

- En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique.

- L'agent qui quitte définitivement la collectivité doit restituer le téléphone portable professionnel.

VIII – LE SMARTPHONE (fourni par l'employeur) le cas d'échéant.

L'arrivée massive des smartphones et des tablettes numériques s'accompagne de modifications organisationnelles du travail des agents publics.

Les règles d'utilisation suivantes doivent être adoptées :

- Le smartphone est un outil de travail dont l'usage personnel peut être autorisé (mention "personnel" pour messages personnels)

- Il n'est pas obligatoire de répondre aux appels ou aux mails en dehors du temps de travail (soir, week-end et congés)

IX – LES BASES LEGALES

L'utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par le Code Général de la Fonction Publique ainsi que par le Code Général des Collectivités Territoriales.

Cette présente partie a pour objectif d'informer les utilisateurs des textes législatifs et réglementaires dans le domaine de la sécurité des systèmes d'information.

A) La Réglementation

- **Loi n° 78-17 du 06/01/1978** sur l'informatique, les fichiers, les libertés.

Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

- **Loi n° 78-753 du 17/07/1978** sur la liberté d'accès aux documents administratifs.

Loi portant diverses mesures d'amélioration entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

- **Loi n° 85-660 du 03/07/1985** sur les droits d'auteur et la protection des logiciels.

Elle interdit à l'utilisateur d'un logiciel toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.

- **Loi n° 91-646 du 10/07/1991** relative au secret des correspondances émises par voie de télécommunication

- **Loi n° 92-597 du 01/07/1992** relative au code de la propriété intellectuelle.

- **Loi n° 2000-230 du 13/03/2000** portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

- **Loi n° 2004-575 du 21/06/2004** pour la confiance dans l'économie numérique.

Elle est destinée à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux.

- **Loi n°2012-410 du 27/03/2012** relative à la protection de l'identité.

B) Le Droit Disciplinaire

- **Décret n°92-1194 du 4 novembre 1992** (art. 6) fixant les dispositions communes applicables aux fonctionnaires stagiaires de la Fonction Publique Territoriale.

- **Décret n°88-145 du 15 février 1988** (art. 36 et 37) relatif aux agents contractuels.

- **Décret n°91-298 du 20 mars 1991** (art. 15) relatif aux agents à temps non complet.

- **Code Général de la Fonction Publique** et notamment ses art. L533-1 à L533-6 et art. L532-7 à L532-10.

C) Le Code Pénal

Code Pénal Livre 3 Titre 2 Chapitre III : Des atteintes aux systèmes de traitement automatisé de données.

- **Article 323-1** :
  « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60.000 euros d'amende.

- **Article 323-2** :
  « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150.000 euros d'amende. »

- **Article 323-3** :
  « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150.000 euros d'amende. »

- **Article 323-4** :
  « La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

- **Article 323-5** :
  « Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
  1º L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26.
  2º L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.
  3º La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.
  4º La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés.
  5º L'exclusion, pour une durée de cinq ans au plus, des marchés publics.
  6º L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés.
  7º L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35. »

- **Article 323-6** :
  « Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.
  Les peines encourues par les personnes morales sont :
  1º L'amende, suivant les modalités prévues par l'article 131-38.
  2º Les peines mentionnées à l'article 131-39.
  L'interdiction mentionnée au 2º de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. »

- **Article 323-7** :
  « La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines. »