CENTRE DE GESTION DE LA
FONCTION PUBLIQUE TERRITORIALE

DÉPARTEMENT D'INDRE & LOIRE

RÉPUBLIQUE FRANÇAISE

EXTRAIT DE REGISTRE
DES DÉLIBÉRATIONS
DU CONSEIL
D'ADMINISTRATION

Séance du 27 juin 2023

N/Réf : BdK/LB 27/06/2023

L'an deux mille vingt-trois, le vingt-sept juin, le Conseil d'Administration du Centre de Gestion, légalement convoqué le quinze mai deux mille vingt-trois, s'est réuni en séance ordinaire dans les locaux de son siège au 25 rue du Rempart à Tours, sous la présidence de Monsieur Jean-Gérard PAUMIER.

Etaient présents :
Mesdames et Messieurs Jean-Gérard PAUMIER, Michel GILLOT, Christian GATARD, Pierre-Alain ROIRON (arrivée 10h06), Sylvia PASCAUD-GAURIER, Jean-Paul ROBERT, Alain ANCEAU, Alain BENARD, Claude COURGEAU, Michèle GASNIER, Michel GUIGNAUDEAU, Gérard HENAULT (arrivée 10h06), Annie LAURENCIN, Patrick LEFRANCOIS, Alain MEDINA, Françoise MORIN, Gérard PERRIER, Bertrand RITOURET(arrivée 10h15)

Etaient absents et excusés :
Mesdames et Messieurs, Isabelle SENECHAL (ayant donné pouvoir à Michel GILLOT), Valérie JADOT (ayant donné pouvoir à Jean-Gérard PAUMIER), Patrick MICHAUD (ayant donné pouvoir à Alain ANCEAU), Pascal BRUN (ayant donné pouvoir à Pierre-Alain ROIRON), Alice WANNEROY (ayant donné pouvoir à Alain MEDINA), Thierry CHAILLOUX (ayant donné pouvoir à Gérard PERRIER), Xavier DUPONT, Elisabeth GRELIER, Martine CHAIGNEAU, Vincent MORETTE.

Assistaient également à la séance :
Monsieur Benoit de KILMAINE, Directeur Général du Centre de Gestion d'Indre-et-Loire,
Monsieur Laurent BEUZIT, Directeur du pôle Administration Générale, Finances du Centre de Gestion d'Indre-et-Loire,
Était absente excusée : Madame Béatrice WACONGNE, Payeuse Départementale d'Indre-et-Loire.

D 2023-048 ACTUALISATION DE LA CHARTE INFORMATIQUE

Le développement des technologies de l'information et de la communication conduit les agents du Centre Gestion à utiliser dans leur travail quotidien l'outil informatique, les réseaux et les services de communication numériques pour l'exécution de leurs missions. Cette utilisation peut comporter un certain nombre de risques à la fois techniques mais également juridiques pouvant engager la responsabilité de la collectivité et de ses agents.

Il appartient au Centre de Gestion en qualité d'institution publique et d'employeur, de garantir la bonne utilisation de ces outils, dans le respect des personnes, de la loi, de la déontologie et de la bonne économie des emplois et des moyens.

La charte jointe en annexe est un code de déontologie interne rappelant les grands axes du cadre légal de la mise à disposition des équipements et moyens mis à disposition des agents et précisant un cadre opérationnel propre à l'administration du système d'information et de communication au sein de l'établissement. Elle définit les conditions d'accès et les règles d'utilisation des ressources informatiques et de communication fournies par le Centre de Gestion. Elle a également pour objet de sensibiliser les utilisateurs aux risques d'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposant le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent, en effet, avoir des conséquences graves de nature à empêcher le bon fonctionnement de l'établissement, voire à engager sa responsabilité civile et/ou pénale, ainsi que celle de la collectivité.

Par conséquent, c'est dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information, mais aussi de respect de la réglementation en vigueur en matière de protection des données, que la charte, ci-après proposée, pose les règles relatives à l'utilisation de ces ressources.

Le Président propose au Conseil d'Administration d'adopter la délibération jointe à ce rapport.

Le Conseil d'Administration,

Vu la directive européenne 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
Vu le règlement n°2016/679 du 27 avril 2016 dit « règlement général sur la protection des données » ;
Vu le code général des collectivités territoriales ;
Vu le Code Général de la Fonction Publique ;
Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;**Vu** la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques

Vu la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique,

Vu la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;
Vu la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles ;
Vu le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques,
Vu le décret n° 2018-687 du 1er août 2018 portant application de la loi n°2018-493 ;
Vu la circulaire du 12 mars 1993 relative aux modalités de l'application de la loi "informatique et libertés" au secteur public, Le guide d'hygiène informatique - Agence nationale de la sécurité des systèmes d'information – Janvier 2017
Vu l'avis du Comité Social Territorial en date du 15 juin 2023;
Considérant les orientations stratégiques arrêtées par la collectivité visant à maintenir l'intégrité de son système d'information ;
Considérant la volonté du Centre de Gestion d'Indre-et-Loire d'être en mesure de garantir un niveau de performance satisfaisant à tous les utilisateurs des ressources informatiques ;

Décide, après en avoir délibéré, à l'unanimité des membres présents ou représentés,

Article 1 : D'adopter la charte informatique, à compter du 28 juin 2023, telle qu'elle est présentée en annexe à la présente délibération.

Article 2 : cette Charte sera communiquée à tous les agents de l'établissement et soumise à leur adhésion sans restriction.

Article 3 : Monsieur le Directeur Général des Services est chargé de prendre toutes mesures nécessaires en vue de l'exécution de la présente délibération.

Fait et délibéré, le 27 juin 2023

Pour expédition conforme,
Le Président du Centre de Gestion
d'Indre et Loire

Jean-Gérard PAUMIER

Acte transmis en Préfecture le : 30/06/2023
Acte reçu en Préfecture le : 30/06/2023
Acte publié électroniquement le : 05/07/2023
ACTE EXECUTOIRE

ANNEXE D 2023-048 ACTUALISATION DE LA CHARTE INFORMATIQUE

CHARTE DES RESSOURCES INFORMATIQUES ET DES SYSTEMES DE COMMUNICATION DU CENTRE DE GESTION D'INDRE ET LOIRE

Préambule :

La présente Charte définit les règles relatives à l'utilisation des différentes ressources et système informatique (SI) mis à disposition par le CDG et tend à sensibiliser les utilisateurs aux risques liés à leur utilisation en termes d'intégrité et de confidentialité des données traitées et de sécurité informatique.

En effet, les agents du Centre de Gestion d'Indre et Loire sont conduits, du fait de leurs missions, à utiliser quotidiennement des outils informatiques et de communication pour l'exercice de leur activité professionnelle.

Ce cadre vise à maintenir les ressources informatiques et de communication à leur plus haut niveau de fiabilité et de performance, en préservant le Centre de Gestion d'Indre et Loire de toute utilisation abusive ou frauduleuse de nature à porter atteinte à l'intérêt et à la continuité du service.

Cette charte, dont l'acceptation et le respect conditionnent l'accès aux différentes ressources précitées, est opposable et donc, applicable, à l'ensemble des utilisateurs des outils informatiques et de communication du Centre de Gestion d'Indre et Loire.

Par **« utilisateur »**, il convient d'entendre toute personne (agents du siège et du service de remplacement lorsqu'ils sont affectés au siège ou en travail à distance, élus, prestataires ou fournisseurs extérieurs, stagiaires, apprentis, etc ...) ayant accès ou utilisant les ressources mises à disposition par le Centre de Gestion d'Indre et Loire.

Par **« outils informatiques et de communication »**, il convient d'entendre l'ensemble des moyens permettant à l'établissement de mettre en œuvre ses missions.

Ces moyens sont :
- Les moyens informatiques et de communication électroniques : le poste de travail fixe ou portable et ses périphériques (écrans, claviers, souris, tablettes graphiques, stockages amovibles, câblage, périphériques, imprimantes simples ou multifonctions, webcam, etc.), les disques durs externes ou internes, cartes mémoire, CD-Rom, clés USB, tablettes, photocopieurs, scanners, etc...
- Les logiciels qu'ils soient en mode SAAS ou hébergés en interne
- Les bases de données
- Les infrastructures
- Le réseau (serveurs, routeurs, systèmes de stockage centralisés, etc ...)
- l'Internet

• les outils communicants : le téléphone (fixe et portable), le fax, les assistants personnels, casques audio, galets audios…

La présente charte s'applique à tous les types d'usage de moyens et de ressources informatiques et numériques, quelle que soit leur fréquence ou leur périodicité et qu'ils aient lieu :
- dans les locaux de l'établissement[1] , quelle que soit leur localisation ;
- dans le cadre d'un usage dit « nomade », quel qu'en soit le lieu ;
- dans le cadre du télétravail et/ou d'un accès distant, quel que soit le lieu de cet accès (domicile, etc.)

Cette charte a fait l'objet d'une information et d'une consultation préalables du Comité Social Territorial qui a donné son avis favorable aux règles ci-dessous rappelées, en date du… juin 2023. Par ailleurs, le présent document est conforme aux recommandations de la Commission Nationale Informatique et libertés[2] (CNIL) et de celles de l'Agence nationale de la sécur**ité des systèmes d'information** (ANSSI).

La charte est communiquée individuellement à chaque utilisateur qui devra s'engager à en connaître et à en appliquer l'ensemble des dispositions.

[1] Les locaux de l'établissement visent son siège social et son annexe dédiée à la médecine du travail, ainsi que le local syndical, sis rue des Tanneurs, à TOURS. Il est rappelé que la présente charte devra notamment être affichée dans tous ces lieux.

[2] **Une Déléguée à la Protection des Données du CDG** veille, au sein du Centre de Gestion d'Indre et Loire, à la bonne application des règles issues de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Sommaire :

Les règles de déontologie applicables aux ressources mises à disposition

Chaque utilisateur est responsable, en tout lieu, de l'usage des ressources informatiques et de communication mises à sa disposition et s'engage à ne pas effectuer d'opérations susceptibles d'avoir des conséquences néfastes sur leur fonctionnement, sur l'intégrité des systèmes d'information et sur la continuité du service proposé par le Centre de Gestion aux collectivités et établissements publics d'Indre et Loire.

Les règles visant à préserver l'intégrité des systèmes et données professionnelles

Les outils informatiques et de communication sont la propriété du Centre de Gestion d'Indre et Loire et ne peuvent être utilisés à des fins extra professionnelles que de manière tout à fait occasionnelle et marginale, et sous condition de ne pas porter atteinte à l'intérêt collectif, ni de mettre en cause la productivité des utilisateurs.

L'utilisation des ressources informatiques doit être **rationnelle** et **conforme à l'intérêt du service**, contribuant ainsi à **éviter sa saturation ou son détournement**. Toute anomalie constatée, susceptible d'affecter la sécurité des ressources doit être signalée immédiatement au prestataire informatique/administrateur systèmes et réseaux.

Le prestataire informatique/administrateur systèmes et réseaux délivre **les droits d'accès** aux systèmes d'information. Tout utilisateur peut demander, sous couvert de son autorité hiérarchique, l'accès aux données et logiciels informatiques attachés à sa fonction.

Les accès sont attribués :
- aux personnels et assimilés dès que leur dossier présente une date d'affectation valide dans le système d'information RH ;
- aux prestataires et partenaires lorsque leur présence est notifiée au Pôle de l'Administration Générale.

L'accès est retiré 15 jours après avoir perdu la qualité au titre de laquelle l'accès leur a été attribué. Toutes les données à caractère privé sont supprimées à l'issue de ce délai, il appartient alors à chaque utilisateur préalablement au retrait de son droit d'accès, de sauvegarder son espace de données à caractère privé.

L'administrateur systèmes et réseaux/prestataire informatique est seul habilité à réaliser ou déléguer toute installation de logiciel. Aucune modification de configuration et rajout de matériel, de programmes ou de copies de logiciels ne doivent intervenir sans l'accord préalable de l'autorité hiérarchique et sous couvert de l'administrateur systèmes et réseaux /prestataire informatique.

L'utilisateur ne doit **pas s'absenter durablement de son poste de travail** en laissant les ressources ou services accessibles. De plus, pour des motifs de consommation d'énergie et de

coûts, il est vivement demandé de se déconnecter et d'arrêter le poste de travail lorsque l'on en n'a plus l'usage.

Tous les fichiers ou dossiers enregistrés sur les outils informatiques du Centre de Gestion d'Indre et Loire sont présumés professionnels. Toutefois, un usage ponctuel et raisonnable des systèmes d'information, à titre exceptionnel, dans le cadre des impératifs et nécessités de la vie personnelle, est toléré. Cette utilisation ne doit pas être contraire à la réglementation en vigueur et ne doit pas mettre en cause le fonctionnement du système informatique de la collectivité. Les données privées devront être identifiées comme telles (Répertoire « *Personnel* » ou « *Privé* ») afin d'être protégées par le droit au respect de la vie privée des utilisateurs. La responsabilité de l'établissement ne pourra être engagée quant à la conservation de ces données.

Les supports amovibles (CD, clé USB, etc.) provenant de l'extérieur doivent être soumis à un contrôle antivirus préalable. L'employeur a accès au contenu d'une clé USB personnelle connectée à l'ordinateur professionnel. Dès lors qu'elle est connectée à un outil informatique mis à la disposition de l'utilisateur par l'employeur, la clé USB est présumée utilisée à des fins professionnelles.

En cas de besoin, en l'absence de l'utilisateur et pour des motifs de continuité de service, ses dossiers professionnels pourront être consultés, dès lors que données professionnelles et privées seront aisément identifiables et différenciables.

Cette autorisation de consultation ponctuelle sur le poste d'un utilisateur absent, fera l'objet d'une demande auprès l'administrateur système et réseaux /prestataire informatique, en accord avec l'autorité hiérarchique. A son retour, l'utilisateur sera informé de cette intervention.

Afin d'assurer la continuité de service, l'utilisateur doit privilégier le dépôt de ses fichiers de travail sur des zones partagées par les membres de son service ou de son équipe. Son supérieur hiérarchique devra s'assurer qu'il a accès aux données professionnelles nécessaires à la continuité de service et prévoir le transfert des données professionnelles de l'utilisateur partant, en concertation avec celui-ci.

Toute information est réputée appartenir à l'établissement à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.

Les règles plus spécifiques d'usage d'Internet, de la messagerie et des réseaux sociaux

Il est rappelé que le réseau Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation de la technologie Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors du Centre de Gestion. Ce dernier met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

Dans le cadre de l'usage d'Internet, ont vocation à être consultés les sites Internet présentant **un lien direct et nécessaire avec l'activité professionnelle**, au regard des fonctions exercées et des missions de chaque utilisateur. Si un **accès raisonnable** dans le cadre des nécessités de la vie courante et familiale est **toléré**, l'accès aux sites non professionnels doit être le plus réduit possible.

L'administrateur systèmes et réseaux /prestataire informatique se réserve la possibilité, sous couvert de la législation en vigueur et à la demande de l'autorité hiérarchique, de limiter à certaines plages horaires l'accès à certains sites non professionnels ainsi qu'aux messageries instantanées. Par ailleurs, il est rappelé que la contribution des utilisateurs à des forums de discussion instantanée, blogs et autres réseaux sociaux non professionnels, est **interdite**.

Tout téléchargement de fichiers, notamment de sons, d'images ou de vidéos, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis au paragraphe 1.3 infra.

L'établissement se réserve le droit de limiter le téléchargement de certains fichiers pouvant présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information, codes malveillants, programmes espions, etc.).

Concernant l'usage de la messagerie (interne et externe), il convient de rappeler que les règles habituelles en matière de communication écrite s'appliquent pleinement à la messagerie : **le message électronique a la même portée juridique qu'un courrier manuscrit** et peut, très rapidement, en quelques clics, être imprimé, communiqué, dupliqué en de nombreux exemplaires à des tiers. Il convient, donc, de respecter un certain nombre de consignes, afin **d'éviter les dysfonctionnements du système d'informations**, de **limiter l'envoi de messages non sollicités** et de **ne pas engager la responsabilité civile et/ou pénale** de Monsieur le Président du Centre de Gestion d'Indre et Loire.

L'envoi de messages électroniques à des tiers obéit aux **mêmes règles que l'envoi de correspondances postales**, en particulier en termes d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer et/ou signer le message, il convient d'en référer au supérieur hiérarchique. Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et leur qualité à recevoir communication des informations transmises.

Les listes de diffusion permettant la réception automatique et périodique d'informations doivent être réservées à un usage strictement professionnel. L'inscription sur une liste de diffusion requiert une autodiscipline des utilisateurs : l'utilisateur doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter l'encombrement inutile de la messagerie, ainsi qu'une dégradation du service.

Un message électronique peut constituer une preuve, ou un début de preuve, engageant l'utilisateur et le Centre de Gestion d'Indre et Loire, au même titre qu'un courrier écrit. Il est demandé, par conséquent, de conserver/archiver tous les messages, envoyés ou reçus, pouvant avoir une valeur contractuelle ou juridique pertinente, en se conformant aux dispositions prévues au tableau de gestion des archives du Centre de Gestion d'Indre et Loire.

Il doit être fait une utilisation de la messagerie conforme aux obligations statutaires des fonctionnaires de **neutralité**, de **loyauté**, de **secret professionnel**, à **l'obligation de réserve** et au devoir de **discrétion professionnelle**.

En tout état de cause, l'envoi de messages électroniques ne peut **en aucun cas se substituer** à toute étude de dossier ou de situation individuelle ou bien encore organisationnelle, des collectivités et établissements publics, qui doivent **impérativement** faire l'objet de courriers signés par Monsieur le Président du Centre de Gestion d'Indre et Loire.

En principe, **un courrier électronique** rédigé et saisi **sur une messagerie professionnelle** est présumé revêtir **un caractère professionnel,** sauf à ce que son contenu intéresse de manière évidente la vie privée de son auteur, dans les aspects que la loi protège de manière privilégiée, à savoir la santé, le patrimoine, ainsi que la vie familiale. Une **utilisation à titre privée est admise,** dès lors qu'elle est raisonnable et qu'elle ne nuit pas au bon fonctionnement du service. Un message électronique doit, alors, pouvoir être identifié comme « *privé* » ou « *personnel* » dans son objet par son expéditeur, ou dans le nom du répertoire d'archivage par son destinataire, pour pouvoir être protégé par le droit au respect de la vie privée et au secret des correspondances.

La loi « Informatique et Libertés » du 6 janvier 1978 modifiée, s'applique également aux messageries en encadrant fortement les modalités de possession de fichiers nominatifs. Il est interdit aux utilisateurs de la messagerie tout stockage, transit, diffusion de documents proscrits par la loi. Par principe, il est formellement interdit de faire circuler, échanger, fusionner des fichiers nominatifs, par la messagerie.

Chaque utilisateur est responsable de l'entretien de sa boîte aux lettres (suppression ou/et archivage de ses messages). Dans un souci de performance du réseau, l'utilisateur doit éviter d'envoyer des messages à un trop grand nombre de correspondants à la fois ou de joindre ou stocker des fichiers de grande taille (supérieurs à 5 Mo) qui ralentissent l'utilisation des réseaux.

En cas de réception de messages non sollicités (spams), et notamment en cas de tentative de phishing visant à obtenir ses identifiants, l'utilisateur veille à :
- ne pas l'ouvrir sans s'être assuré préalablement de son innocuité ;
- ne pas y répondre ;
- ne pas le transférer ;
- en informer sans délai l'administrateur systèmes et réseaux/prestataire informatique.

Pour préserver le bon fonctionnement des services, des limitations pourront être mises en place. En particulier des solutions de traitement des messages indésirables (spam, contrôle des virus, ...) seront déployées.

Concernant les réseaux sociaux, ceux-ci permettent aux utilisateurs de créer de nouvelles relations professionnelles et d'optimiser les échanges professionnels autour de leurs projets. Ils présentent, néanmoins, des risques et sont susceptibles d'engager la responsabilité, notamment, en termes d'image, ou de fraude. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées.

Dans le cadre de la sphère professionnelle, l'utilisateur doit obtenir au préalable l'autorisation de son supérieur hiérarchique pour pouvoir participer à un réseau social et/ou créer un espace sur un réseau social au nom de sa structure. Si l'autorisation a été donnée, l'utilisateur doit se conformer aux règles et instructions édictées par son supérieur hiérarchique, ce dernier étant seul compétent pour déterminer les conditions d'utilisation du réseau social.

Lorsqu'un réseau social est utilisé à des fins professionnelles, l'utilisateur devra :
- s'abstenir de publier un contenu de façon anonyme et, au contraire, s'identifier clairement, en précisant sa fonction au sein de l'établissement ;
- répondre aux contributions des tiers avec pertinence, exactitude, en s'efforçant de promouvoir l'image de l'établissement ;
- respecter les conditions générales d'utilisation du réseau social et l'ensemble des lois applicables (notamment en matière de concurrence, de consommation et de propriété intellectuelle, de droit de la presse, de propos illicites) ;
- utiliser uniquement les outils de communication de l'établissement, selon les instructions qui lui ont été données ;
- s'abstenir de diffuser toute information confidentielle ou sensible relative à l'établissement ou à ses partenaires ;
- prendre toutes les précautions utiles pour que son utilisation des réseaux sociaux soit sans danger pour les systèmes d'information et de communication de l'établissement.

Les règles d'ordre public visant à respecter les droits de la propriété intellectuelle et les droits d'auteurs

L'utilisation des systèmes d'information et de communication de l'établissement implique le respect des droits de propriété intellectuelle et du droit à l'image.

Sans que cette liste soit exhaustive, l'utilisateur s'engage à :
- utiliser les logiciels et applications, dans les conditions souscrites par l'établissement ;

- ne pas effectuer de copie illicite de logiciels ou d'applications et, a fortiori, de stocker et/ou tenter d'installer des logiciels ou applications pour lesquels l'établissement ne possèderait pas un droit d'usage/licence ;
- ne pas reproduire, copier, utiliser remettre à des tiers ou diffuser, les bases de données, pages web, dessins, modèles, logos ou autres créations de l'établissement ou de tiers protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- ne pas reproduire, copier ou diffuser des textes, des images, des photographies, des œuvres musicales, audiovisuelles ou multimédia et, plus généralement, toute création ou invention provenant du réseau internet, d'applications web ou mobiles, sans autorisation ou licence ;
- ne pas reproduire, copier, utiliser ou diffuser des éléments susceptibles de porter atteinte à l'image ou à la vie privée des utilisateurs ou de tiers à l'établissement.

La plupart des données circulant sur Internet sont protégées par un droit de propriété intellectuelle ou d'auteur. L'article L 122. 5 du Code de la propriété intellectuelle n'autorise que les « copies ou reproductions [d'une œuvre] strictement réservées à un usage privé et non destinées à une autorisation collective » et « sous réserve que soient clairement indiqués le nom de l'auteur et la source, les analyses et courtes citations » dans un but d'exemple ou d'illustration. En conséquence, la diffusion, voire le simple enregistrement, d'œuvres ou de données contrevenant à la législation existante ou sans l'autorisation des titulaires des droits, peut faire l'objet de poursuites pénales ou civiles. Il convient, donc, de privilégier les ouvrages ou données dont la copie est libre.

Ces règles sont applicables pour **tout type de document**.

Les règles d'ordre public visant à garantir la confidentialité et la sécurité des informations

L'utilisateur est responsable de ses fichiers, de l'intégrité de son espace de travail et de l'utilisation qu'il fait des ressources mises à sa disposition par le Centre de Gestion.

Il doit **assurer la protection de ses informations et données**, en utilisant les différents moyens de sauvegarde individuels ou collectifs mis à sa disposition.

Il doit **signaler toute tentative de violation de son compte** (Nom d'utilisateur + mot de passe) et, de façon plus générale, **toute anomalie** qu'il peut constater.

L'utilisateur **ne doit ni lire, ni copier, ni tenter de lire ou copier les fichiers** d'un autre utilisateur sans son autorisation. De même, il **ne doit ni intercepter ni tenter d'intercepter les communications privées** entre utilisateurs (messageries, en particulier). Il ne doit pas usurper une autre identité. Il lui est, en particulier**, interdit d'utiliser une session ouverte par un autre utilisateur** (sauf accord explicite) et non refermée par lui. Il doit, au préalable, clore une session avant d'en ouvrir une autre à son nom.

Enfin, l'utilisateur devra modifier régulièrement son mot de passe tel que le système le lui permet.

Plus généralement, une attention toute particulière est requise dans l'utilisation des outils de travail « nomades » (clé USB, ordinateur portable, disque dur externes ou tout autre support) afin d'éviter tout vol ou/et perte de données.

Les utilisateurs sont toutefois informés que l'administrateurs systèmes et réseaux/ prestataire informatique est conduit, en raison de ses fonctions et selon des procédures déterminées, à avoir accès à l'ensemble des informations relatives aux utilisateurs (messages, connexions à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail. Néanmoins, l'administrateur système et réseaux /prestataire informatique est tenu au secret professionnel et ne peut utiliser ses droits d'administrateur qu'à des fins strictement professionnelles.

Les règles d'ordre public relatives au traitement des données nominatives et/ou personnelles

Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de collecte et de traitements automatisés ou manuels de données à caractère personnel, prévues pour l'essentiel dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés » en vigueur, dans le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 et dans la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

Les données à caractère personnel sont des informations qui permettent – sous quelque forme que ce soit – directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent. Leur collecte doit se faire dans le cadre d'une finalité définie et limitée au strict nécessaire.

Les traitements de données à caractère personnel consistent en toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, …).

Les utilisateurs s'engagent à ce que seules les données strictement nécessaires à leur activité professionnelle soient collectées. Pour toute question relative à l'utilisation, au traitement et/ou la protection de leurs données, les utilisateurs peuvent s'adresser au Délégué à la Protection des Données du Centre de Gestion à l'adresse suivante vpelletier964@gmail.com.

Par ailleurs, chaque personne concernée par un traitement de ses données personnelles peut demander l'exercice de ces droits, notamment en contactant le Délégué à la protection des données (DPO) à l'adresse précitée. Elle dispose également d'un droit de réclamation auprès de la CNIL.

Le Centre de Gestion déclare se conformer à la procédure en vigueur pour la collecte et la mise en œuvre d'un traitement de données à caractère personnel.

Le guide du « bon usage » des différents réseaux informatiques et de communication du Centre de Gestion d'Indre et Loire

Les clés de l'accès aux ressources informatiques : login/identifiant et mots de passe

L'accès aux ressources informatiques du Centre de Gestion d'Indre et Loire sur site et à distance se fait via un couple d'identifiant / mot de passe. Ces couples identifiant / mot de passe engagent l'agent dans l'usage informatique des moyens à sa disposition (usage interne ou à distance, Internet, fichiers, etc ...). Ces informations sont individuelles et confidentielles et ne doivent pas être communiquées.

L'utilisateur doit veiller à ne pas quitter son poste de travail (que ce soit sur site et, à plus forte raison, en télétravail) en laissant des ressources ou services accessibles et penser à se déconnecter ou à verrouiller la session.

En cas d'absence prolongée ou momentanée d'un agent, sur demande de l'autorité hiérarchique, pour assurer une continuité de service, et pour des besoins de maintenance informatique (installation de logiciels, dépannage), le mot de passe d'ouverture d'une session pourra être réinitialisé pour la durée de l'intervention, afin d'accéder à une session sur le poste de travail. L'utilisateur sera alors informé par l'administrateur systèmes et réseaux/prestataire informatique de la réinitialisation de son mot de passe.

Le mot de passe devra être changé aussi régulièrement que le système d'information le requière et respecter une complexité imposée par le système (exemple : choix d'un mot de passe de 5 caractères mini., composé de lettres majuscules et minuscules, de chiffres et de caractères spéciaux afin d'être difficilement devinable).

Lorsque l'agent quitte la collectivité, il devra prendre toutes les mesures nécessaires afin de permettre une continuité dans l'activité du service, au regard des données informatiques professionnelles de son poste de travail.

En cas de perte, de vol, ou de suspicion de compromission de ses moyens d'authentification, l'utilisateur est tenu d'en aviser sans délai l'administrateur systèmes et réseaux/prestataire informatique en suivant, le cas échéant, la procédure formalisée permettant d'invalider et/ou de renouveler ses moyens d'authentification. Cet acte d'information est de nature à dégager la responsabilité de l'utilisateur pour les agissements qui auraient lieu après sa déclaration.

Les réseaux et les bases de données

Le réseau du Centre de Gestion d'Indre et Loire est constitué d'un ensemble d'éléments tels que les serveurs, switches et postes de travail. Ces éléments sont dimensionnés pour répondre aux besoins des agents, et permettre les échanges de flux de façon optimale. Seul

l'administrateur systèmes et réseaux/prestataire informatique, dans le but d'améliorer les transmissions ou de résoudre des problèmes techniques est habilité à « écouter » le réseau et à en analyser le contenu. Toute pollution du réseau par le biais d'applicatifs, toute « écoute » hors de ce contexte est strictement interdite et entrainerait des sanctions envers l'agent émetteur.

Sont considérées comme des bases de données, l'intégralité des documents contenant des listes, mots de passe, codes d'accès, informations à caractère personnel et confidentiel. L'accès aux bases de données du Centre de Gestion d'Indre et Loire est limité aux seuls propriétaires et utilisateurs désignés de ces bases, dans le cadre de leur exploitation et de leur maintenance. Les informations présentes dans ces bases de données ne peuvent être diffusées à l'extérieur du Centre de Gestion d'Indre et Loire et sont couvertes par la règle du secret professionnel.

Toute base de données contenant des données à caractère personnel permettant l'identification directe ou indirecte d'une personne doit faire l'objet d'une déclaration d'utilisation auprès de la CNIL, et les personnes en relevant doivent être informées de leur droit d'accès et de rectification des informations stockées les concernant (voir supra point 1.5).

Le Centre de Gestion met à disposition une architecture réseau permettant le stockage, la sauvegarde et la restauration de fichiers informatiques facilitant le fonctionnement des services. Par conséquent, l'ensemble des fichiers professionnels détenus par chaque utilisateur doit être prioritairement stocké sur le réseau à disposition.

Par ailleurs, le Centre de gestion met à disposition un portail web qui offre aux agents itinérants et aux agents en télétravail un accès aux applications et aux ressources internes dont ils ont besoin sans avoir à installer le moindre logiciel. Ce portail est accessible depuis n'importe quel navigateur et depuis n'importe quel ordinateur relié à Internet. L'utilisation du portail depuis un ordinateur partagé dans un espace public est interdite.

Afin d'accéder à certaines applications métiers, les utilisateurs peuvent être amenés à utiliser un VPN pour sécuriser les échanges de données entre le poste informatique et le réseau du Centre de gestion.

Les messageries (internes et externes) et le courrier électronique en général

Le Centre de Gestion d'Indre et Loire met à disposition de chaque agent une adresse de messagerie générique, identifiée par service, et se réserve, dans le cadre de l'évolution du système de messagerie, d'y adjoindre une adresse de messagerie individuelle, sous le format prénom.nom@cdg37.fr. Ces messageries, également accessibles sur le réseau internet et sur le Web via le portail précité, sont **destinées à un usage professionnel**, en respectant le principe d'utilisation et le cadre imposés par les échanges écrits afin de ne pas engager indument la responsabilité du Centre de Gestion En effet, la messagerie ne se substitue pas

au courrier « papier » notamment lorsque le contenu du message doit comporter le visa de l'autorité territoriale ou de la personne habilitée à cet effet, conformément aux délégations de signature prévues.

L'usage personnel, à titre ponctuel et modéré de la messagerie, est toléré. Cet usage devra alors être clairement identifié comme tel, en mentionnant dans l'intitulé de l'objet du message « Personnel » ou « Privé ». Pour assurer et maintenir l'équilibre du réseau du Centre de Gestion d'Indre et Loire, la messagerie ne devra pas être utilisée pour des envois de documents dont la taille est supérieure à 5 Mo vers l'extérieur. En cas d'envoi de taille supérieure, les agents devront privilégier l'usage de la plateforme d'échanges sécurisée du Centre de Gestion. Il incombe, en conséquence, à chacun de gérer l'archivage de sa messagerie. Par ailleurs, chaque utilisateur gère librement les messages d'absence sur son adresse nominative pendant ses congés.

L'usage des messageries personnelles au sein du Centre de Gestion d'Indre et Loire est toléré, de manière ponctuelle et limité dans le temps. Aucun fichier, aucun document du Centre de Gestion d'Indre et Loire, aucune information contenue dans les bases de données, ne doit transiter par ces messageries personnelles qui engagent la responsabilité de leur utilisateur en cas de diffusion à des tiers, même involontaire, de données personnelles, confidentielles, ou soumises à l'obligation de discrétion.

En cas d'absence inopinée ou prolongée ou de départ d'un agent, et afin de ne pas interrompre la continuité du service, le prestataire informatique pourra transmettre tout message issu de la messagerie de l'agent concerné, non identifié comme personnel ou privé dans son objet.

L'utilisation d'Internet

Le Centre de Gestion d'Indre et Loire permet aux agents identifiés de bénéficier d'un accès Internet. Cet accès est filtré et géré par l'administrateur des systèmes et réseaux/prestataire informatique. La visite de sites à caractère interdit par la loi est proscrite. Un agent ne peut être tenu pour responsable s'il reçoit, à son insu, des documents émanant de tels sites ou bien encore, s'il accède involontairement à l'un de ces sites. Il devra, néanmoins, immédiatement en faire part à l'administrateur des systèmes et réseaux/prestataire informatique.

Pour garantir un niveau d'accès suffisant à la ressource Internet, l'autorité hiérarchique peut décider de bloquer ou limiter l'accès à d'autres sites.

L'historique des connexions Internet sera conservé pendant une durée de **12 mois** et ne sera accessible que sur une demande spécifique d'un juge d'instruction ou d'un officier de police judiciaire dans le cadre d'une instruction judiciaire (article 97 du Code de Procédure Pénale).

L'usage d'Internet doit se conformer aux règles en vigueur au sein du Centre de Gestion d'Indre et Loire. L'accès pour des raisons personnelles doit être ponctuel et limité dans le temps.

L'utilisation des accès mobiles Internet

Tout équipement mobile (ordinateur portable, téléphone portable) du Centre de Gestion permet d'accéder à Internet par des moyens de connexion extérieurs (points d'accès sans fil, carte 3G, etc ...). L'agent en charge de cet équipement mobile doit alors s'assurer que tous les moyens sont mis en œuvre pour protéger l'équipement (pare feu, antivirus, etc ...). Les connexions simultanées au réseau interne au Centre de Gestion et à Internet par un moyen extérieur sont interdites pour des raisons de sécurité.

Seules les solutions VPN (connexion sécurisée entre l'équipement informatique d'un utilisateur et le réseau informatique de l'organisation à laquelle il appartient) fournies et installées par l'administrateur des systèmes et réseaux/prestataire informatique sont autorisées.

L'utilisation des ressources téléphoniques

Le Centre de Gestion d'Indre et Loire met à disposition des agents un ou plusieurs moyens téléphoniques (fixes et mobiles). L'usage du téléphone à titre privé est admis à condition de demeurer exceptionnel.

Il convient de privilégier, pour les agents disposant d'un téléphone « fixe », les appels vers les téléphones fixes et les numéros non surtaxés. Les appels vers les mobiles extérieurs à ceux du Centre de Gestion d'Indre et Loire devront avoir une durée limitée dans le temps et se justifier par une réelle nécessité.

Les appels vers les numéros de mobile, pour les agents disposant d'un téléphone mobile de service, seront en priorité émis depuis ces mobiles.

En cas de perte ou de vol, il convient d'avertir au plus tôt l'autorité territoriale.

L'utilisation de logiciel de pointage *(le cas échéant)*

Un logiciel de pointage de présence est susceptible d'être mis en place pour assurer le suivi des horaires de travail des agents. Ce dispositif sera préalablement présenté au CST du Centre de Gestion puis, porté à la connaissance des utilisateurs.

Les conditions d'utilisation spécifiques

1.1.1 La mobilité et l'accès distant

Dans le cadre de ses déplacements professionnels, quelle que soit leur durée ou leur fréquence, l'utilisateur assure la garde et la responsabilité des systèmes d'information et de communication qui lui sont confiés. Il a, dans cette hypothèse un niveau de surveillance et de confidentialité renforcé et doit veiller à ce que des tiers non autorisés ne puissent accéder à ses moyens ni les utiliser.

Ainsi, l'utilisateur se doit d'adopter une attitude de prudence et de réserve renforcées au regard des informations, données et ressources du système d'information de l'établissement

qu'il pourrait être amené à manipuler ou à échanger à l'extérieur de l'enceinte de la collectivité. La connexion à des points d'accès Wi-Fi publics qui ne sont pas de confiance (par exemple à l'hôtel, la gare ou l'aéroport...) est proscrite. L'utilisateur devra se connecter par le biais des clés 3G/4G ou téléphone (via la fonction de partage de connexion) professionnel mis à disposition.

En cas de dysfonctionnement, de blocage, de perte ou de vol de l'équipement, les utilisateurs doivent en informer immédiatement l'autorité territoriale. Ils doivent par ailleurs assister la collectivité, dans toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

1.1.2 Le télétravail

L'utilisateur en situation de télétravail se doit de respecter les conditions d'utilisation usuelles et professionnelles du matériel informatique mis à sa disposition. De son côté, le Centre de Gestion fournira (si nécessaire) le matériel et l'accès aux logiciels en garantissant la sécurisation des données, tels que prévus par la Charte du télétravail au Centre de Gestion. Les conférences téléphoniques et les visioconférences répondant à des nécessités de service et d'activité sont soumises à une obligation de confidentialité.

Le Centre de Gestion apportera à chaque agent télétravailleur les mêmes conditions de travail qu'en présentiel. En revanche, ne sont pas fournis, dans le cadre du télétravail, d'équipement de reprographie et de téléphonie mobile type téléphone portable et abonnement pour des raisons techniques et de sécurité. En conséquence, la configuration de l'équipement remis se compose :
- D'un ordinateur portable,
Un équipement « spécifique » pourra être demandé et attribué au cas par cas, selon la nature de l'activité et des missions.

Les logiciels et/ou applications métiers seront mis à disposition selon les données à traiter, le fonctionnement du logiciel ou application et les tâches à effectuer.

L'agent télétravailleur s'engage à prendre les appels entrants via le logiciel de communication spécifique du Centre de Gestion (type VPN). Il continue ainsi d'être disponible et joignable sur son numéro professionnel pendant son temps de télétravail pour son employeur et/ou les usagers et/ou les collaborateurs sans pouvoir vaquer à ses occupations personnelles et/ou familiales. Il devra faire un transfert d'appel de sa ligne professionnelle sur le téléphone portable qu'il aura soit à titre professionnel pour les agents qui en sont détenteurs, soit sur leur téléphone personnel. Des outils d'aide au travail collaboratif type Microsoft Teams pourront être utilisés pour les communications effectuées à partir du domicile afin de préserver l'anonymat en cas d'utilisation de la ligne personnelle.
En cas de refus cela pourra justifier un refus d'éligibilité au télétravail par la hiérarchie.

Le Centre de Gestion reste propriétaire de l'équipement fourni dans le cadre du télétravail. Il appartient à l'agent d'en assurer une bonne conservation et l'utilisation dans le respect des règles de sécurité des systèmes d'information et de protection des données. En cas de

dysfonctionnement, l'agent télétravailleur doit contacter l'administrateur systèmes et réseau/prestataire informatique en créant un ticket sur l'Espace Numérique de Travail (ENT). Si le problème perdure, l'agent télétravailleur doit se rendre auprès des services afin de faire réparer le matériel. Toutefois, l'établissement peut autoriser l'utilisation de l'équipement informatique personnel de l'agent (partiellement ou complètement).

Le télétravailleur s'engage à respecter la législation en vigueur ainsi que les règles fixées par la présente Charte en matière de sécurité informatique (confidentialité, mot de passe, protection des données...). Il doit préserver la confidentialité des accès et des données, éviter toute utilisation abusive ou frauduleuse des outils mis à sa disposition. Le télétravailleur s'engage à ne pas sous-traiter les travaux qui lui sont confiés par son supérieur hiérarchique, à respecter la confidentialité des informations obtenues ou recueillies dans le cadre de son travail à domicile. Le matériel doit être réservé à un usage professionnel et ne peut être utilisé que par l'agent lui-même.

Le télétravailleur s'engage à prendre soin des équipements confiés et en assure la bonne conservation. Il est responsable de l'intégrité du matériel mis à sa disposition et notamment des données qui y sont stockées. En cas de perte ou de vol et en cas de panne ou de mauvais fonctionnement des équipements de travail mis à disposition, le télétravailleur doit en aviser immédiatement l'autorité territoriale suivant la procédure en vigueur.

Les biens du Centre de Gestion étant couverts en tous lieux, les équipements mis à disposition des agents dans le cadre du télétravail sont bien couverts à leur domicile, tant au titre de la garantie « Dommages aux Biens » que de la garantie « Responsabilité Civile » pour les dommages qu'ils pourraient occasionner notamment aux locaux. Les risques liés aux équipements informatiques fournis sont donc couverts par l'assurance de l'établissement de la même façon lorsque l'agent est en télétravail que lorsqu'il est sur son lieu d'affectation. L'agent doit donc y veiller personnellement de la même façon quel que soit son lieu de travail.

Les responsabilités du Centre de Gestion d'Indre et Loire et les moyens de contrôle pour un usage légal des ressources

En sa qualité d'employeur, le Président du Centre de Gestion de la fonction publique territoriale d'Indre et Loire est **responsable des faits commis par ses agents au moyen des outils informatiques et de communication[3] mis à leur disposition**. Il est, par conséquent, formellement exclu que ces outils puissent faciliter la réalisation de manquements aux obligations statutaires ou d'infraction de droit commun.

Dans le cadre de cette responsabilité, et à la condition de détenir des présomptions sérieuses d'infraction aux règles énoncées dans la présente charte, le CDG37 pourra être amené à **contrôler la légalité de l'utilisation de ces outils, dans un souci d'assurer la sécurité des systèmes d'information et non pas de réaliser un contrôle individuel de l'activité des utilisateurs**. A cet effet, l'administrateur systèmes et réseaux/prestataire informatique,

[3] Article 1384 du Code Civil. Articles 226-16 à 226-24 du Code Pénal.

mandaté par l'autorité hiérarchique, consignera dans un registre spécifique toute intervention en rapport avec de tels contrôles.

Chaque utilisateur doit prendre conscience des risques qu'il peut faire courir à la collectivité par un mauvais usage des outils mis à sa disposition **:**

- Des risques techniques (encombrement des réseaux, possibilités d'intrusions de l'extérieur et malveillance de l'intérieur, attaques virales …) ;

- Des risques juridiques pour la collectivité mais, également, pour les utilisateurs eux-mêmes ;

- Des risques financiers (un usage mal maîtrisé peut entrainer des conséquences financières importantes, en termes de coûts et de perte de temps de travail).

Afin de limiter ces risques seront, notamment, surveillées et conservées pendant une durée de **12 mois**, dans le respect de la législation applicable et, notamment, de la loi sur l'informatique et les libertés du 6 janvier 1978 modifiée, les données relatives :

- Au contenu des fichiers et messages à caractère professionnels (sauf les fichiers identifiés par l'agent comme « Personnel» ou « Privé » contenus sur le disque dur de l'ordinateur mis à sa disposition, qui ne pourront être contrôlés qu'en présence de l'agent ou une fois celui-ci dûment averti). **Le contenu des messages à caractère « personnel » ou « privé »** des utilisateurs **ne peut en aucun cas être contrôlé**) ;

- A l'utilisation des logiciels applicatifs, pour contrôler l'accès, la modification et la suppression de fichiers ;

- Aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter toute anomalie liée à l'utilisation de la messagerie et surveiller les tentatives d'intrusions et les activités telles que la consultation de sites web illicites (nature et durée des connexions) ou le téléchargement de fichiers, logiciels ou autres documents dont l'origine n'est pas garantie ou illicite.

Il convient de préciser, concernant la messagerie, que des outils permettent de vérifier la « fiabilité informatique » d'un message, principalement contre les virus et « spam », sans en visualiser le contenu. En cas de doute, l'autorisation du destinataire devra être sollicitée avant l'ouverture de tout message. Par ailleurs, l'administrateur systèmes et réseaux/prestataire informatique contrôle la taille des boîtes aux lettres pour éviter l'engorgement du système et maîtriser le volume des données. La taille limite d'une boîte sur les serveurs de messagerie est en général de 50 Mo. Un système d'alerte invite les utilisateurs dont la boîte devient trop volumineuse à en alléger le contenu.

Par ailleurs, il pourra être procédé au blocage de l'accès à certains sites considérés comme dangereux ou interdits ou n'ayant aucun lien avec le domaine professionnel, au regard de leur

contenu présumé (sites à caractère pornographique, pédophile, d'incitation à la haine, révisionniste, etc ...). Toute mesure de blocage fera l'objet de l'information des utilisateurs au moyen d'un message type.

De même, pour répondre à des nécessités de maintenance et gestion techniques des installations, et non pas de contrôle individuel, l'utilisation des ressources téléphoniques pourra être analysée et contrôlée dans le respect de la législation applicable et, notamment, de la loi sur l'informatique et les libertés du 6 janvier 1978 modifiée. Les agents sont informés de l'enregistrement et la conservation pour une durée de 3 mois à compter de l'enregistrement du numéro appelé, des informations suivantes :

- L'identité de l'utilisateur du poste (nom, prénom, numéro de poste) ;
- La communication téléphonique : numéro de téléphone appelé, nature de l'appel (local, national, international), la durée, la date, l'heure de début et de fin d'appel. Le traitement de telles informations a pour but la gestion de l'annuaire interne, la maîtrise des dépenses téléphoniques et l'établissement de statistiques. **Lorsque des relevés justificatifs des numéros appelés sont établis, les quatre derniers chiffres de ces numéros sont occultés conformément à la réglementation CNIL** (sauf en cas d'utilisation manifestement anormale, librement appréciée par l'autorité hiérarchique).

Ces données sont susceptibles d'être analysées par le seul administrateur système et réseaux/prestataire informatique, à la demande expresse de l'autorité hiérarchique.

L'employeur pourra produire des relevés justificatifs de numéros appelés pour établir une utilisation personnelle abusive du poste mis à disposition de l'agent, lequel pourra demander à avoir communication des numéros de téléphone complets des correspondants appelés à titre personnel. Les mêmes dispositions s'appliquent lorsqu'il est demandé à l'agent le remboursement du coût d'une ou plusieurs communications téléphoniques regardées comme passées à titre privé ou abusif.

Aucun enregistrement, ni écoute des conversations n'est réalisé.

Concernant les téléphones portables mis à disposition de certains agents, leur temps de fonctionnement est forfaitaire. Il convient de rappeler qu'un soin tout particulier doit être apporté à ce type d'équipement fragile et facile à dérober (il est indispensable, lors de la première utilisation de l'appareil, de penser à changer le code PIN). Rappelons, par ailleurs, que **son usage en conduisant** est non seulement **dangereux,** mais **strictement interdit**.

En application de l'article L121-8 du Code du travail et l'article 32 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ***aucune information concernant directement un utilisateur des systèmes d'information du Centre de Gestion d'Indre et Loire,***

ne peut être collectée par un dispositif qui n'a pas été préalablement porté à sa connaissance.

Le rôle de l'administrateur systèmes et réseaux / prestataire informatique

Outre les **moyens techniques** (information et communication) mis à disposition des agents du Centre de Gestion d'Indre et Loire, ces derniers pourront également bénéficier de **moyens humains** pour assurer la sécurité et le bon fonctionnement de ces moyens techniques, **en la personne de l'administrateur systèmes et réseaux/responsable informatique**.

D'une manière générale, l'administrateur système et réseaux/responsable informatique a le droit de faire **tout ce qui est nécessaire pour assurer le bon fonctionnement des différents outils** informatiques et téléphoniques sous le contrôle et à la demande expresse de l'autorité territoriale. Aucune exploitation des données collectées, à des fins autres que celles liées au bon fonctionnement et à la sécurité du système d'information, ne peut être opérée, sur ordre de l'autorité hiérarchique.

L'administrateur systèmes et réseaux/responsable informatique est **tenu au secret professionnel** et a **une obligation de discrétion renforcée** pour toutes les informations qu'il aurait été amené à connaître dans le cadre de ses fonctions. Il peut saisir l'autorité hiérarchique d'un utilisateur, en cas de non-respect des règles énoncées dans la présente charte.

- Il **assure et maintient la sécurité** du système par l'installation et la mise à jour du système d'exploitation des postes de travail et serveurs.
- Il **accompagne les agents dans l'utilisation** des moyens informatiques et de communication par la formation, l'assistance pour résolution de problèmes techniques et l'information des contraintes de service.
- Il **intervient sur les outils** en cas de force majeure, à ce titre il peut avoir à examiner des fichiers ou des courriers afin d'obtenir suffisamment d'informations pour diagnostiquer et corriger des problèmes avec les logiciels ou pour déterminer si un utilisateur agit en violation des règles énoncées plus haut. Il interviendra toujours en ayant, préalablement informé l'agent, et ce, à l'exclusion de l'accès aux répertoires, fichiers et messages clairement identifiés ou expressément signalés comme lieux de stockage de données personnelles.
- Il **analyse les différents éléments sources de problèmes techniques**, les éléments relatifs aux flux de trafic et aux volumes stockés et, notamment :

  - les fichiers stockés (format, date, taille, etc ...),

  - les ressources matérielles et logicielles,

- les connexions au réseau (identifiants, date et heures de connexions, etc ...),

- les échanges via le réseau,

- les connexions Internet (identifiant de connexion, volume de données transférées, date et heure de connexion, etc ...),

- les messages stockés (fréquence, taille des fichiers transmis, etc ...).

Dans ce cadre, la confidentialité des données sera systématiquement respectée. L'administrateur systèmes et réseaux est soumis à un strict devoir de réserve et de secret professionnel.

Les sanctions en cas de manquement aux règles et mesures de sécurité de la charte

Les manquements aux règles et mesures de sécurité énoncées dans la présente charte sont susceptibles d'engager la responsabilité de l'utilisateur et d'entraîner, à son encontre, **des avertissements, des limitations ou suspensions** dans l'utilisation de tout ou partie du système d'information et de communication, voire **des sanctions disciplinaires** proportionnées à la gravité des manquements reprochés ou encore des **poursuites judiciaires,** en fonction de la nature et de la gravité des faits reprochés et de leurs conséquences sur le préjudice subi par le Centre de Gestion d'Indre et Loire.

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

Elle entre en vigueur à compter du ... 2023.

Faite à TOURS, le

Le Président du Centre de Gestion d'Indre-et-Loire

Jean-Gérard PAUMIER

ANNEXE : Liste des textes juridiques de référence (non exhaustive)

- La Directive n°96/9CE du 11 mars 1996 concernant la protection juridique des bases de données
- La Directive n° 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)
- La loi Informatique et libertés du 6 janvier 1978 modifiée par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;
- La loi du 30 septembre 1986 portant sur la réglementation des télécommunications ;
- La loi du 5 janvier 1998 visant à lutter contre la fraude informatique ;
- La loi du 3 juillet 1985 et le décret du 27 avril 1994 sur la propriété intellectuelle ;
- La loi du 21 juin 2004 relative à la confiance dans l'économie numérique ;
- Le Code Général de la Fonction Publique
- Le Code pénal (art. 226-16 à 226-24 relatifs aux atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques ; art. 323-1 à 323-7 relatifs aux atteintes aux systèmes de traitement automatisé de données)
- Le Code de procédure pénale (articles 323-1 à 323-7) ;
- Le Code du travail ;
- Le Code de la propriété intellectuelle ;
- Le Code des postes et communications électroniques ;
- L'Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;
- Le Décret n°2005-1309 du 20 octobre 2005 relatifs aux mesures générales d'application de la loi "informatique et libertés";
- La Circulaire du 12 mars 1993 relative aux modalités de l'application de la loi "informatique et libertés" au secteur public ;
- Le Rapport de la CNIL du 5 février 2002 mis à jour en février 2004 sur la cybersurveillance sur les lieux de travail.

Adhésion à la Charte du bon usage des ressources informatiques et de communication du Centre de Gestion d'Indre et Loire :

Je, soussigné(e), ..., reconnais **avoir pris connaissance** des dispositions de la Charte du bon usage des ressources informatiques et de communication du Centre de Gestion d'Indre et Loire, **y adhérer** pleinement et déclarer **m'y conformer***.

Je m'engage en particulier à :

· ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
· ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
· ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
· prendre toutes les mesures conformes aux usages dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
· prendre toutes précautions conformes aux usages pour préserver la sécurité physique de ces données ;
· m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
· en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

J'ai pris connaissance du fait qu'une utilisation fautive de ces ressources pourrait m'exposer à des sanctions disciplinaires et, le cas échéant, à des poursuites pénales.

Faite à TOURS, le .....

Signature

Fait en 2 exemplaires : 1 pour l'intéressé(e)
1 pour la collectivité

**Le contenu de cette charte est susceptible de connaître des évolutions en fonction du cadre législatif en vigueur ainsi que du contexte technologique, en évolution constante et rapide en matière de technologies de l'information.*