Charte d'utilisation des moyens de communication électronique et des systèmes d'information au sein de la Région Hauts-de-France

Référence : **2018.04-CHARTE-SMSI/27002-5**

SOMMAIRE

1 PRÉAMBULE

La Région Hauts-de-France met en œuvre un système d'information et de communication nécessaire à l'exercice de ses missions. Elle met ainsi à disposition de ses agents et collaborateurs des moyens de communication électronique, ressources informatiques, téléphoniques, informationnelles, numériques et technologiques.

Ces différents outils offrent également à leurs utilisateurs une ouverture vers l'extérieur, et se révèlent des vecteurs de modernisation de la **Collectivité** et du service public si leur utilisation est faite à bon escient et dans le respect des usages et de la législation en vigueur.

A l'inverse, une mauvaise utilisation de ces outils peut engendrer des risques d'atteinte à la confidentialité, à la disponibilité et à l'intégrité de l'information (virus, intrusions sur le réseau interne, vols de données Le risque majeur d'un mauvais usage peut entrainer des interruptions de service sérieuses jusqu'au blocage total du fonctionnement de la collectivité. Par ailleurs, cela peut également entrainer des conséquences graves de nature à engager la responsabilité civile et / ou pénale de l'utilisateur ainsi que celle de la **Collectivité** (atteintes aux droits de la personne résultant des fichiers de données à caractère personnel, atteintes aux droits d'auteur…).

La présente Charte s'inscrit dans une démarche d'information, de sensibilisation, de responsabilisation des **utilisateurs** des **moyens de communication électronique** et du système d'information de la Région Hauts-de-France.

Elle définit les grands principes applicables aux moyens de communication électronique et des systèmes d'information. Elle sera agrémentée de dispositions particulières s'intégrant à la présente Charte, de déclinaisons thématiques, guides de bonnes pratiques, notes techniques et de service, principes d'utilisation, procédures relatives à leur mise en œuvre en fonction des évolutions des outils et services mis à disposition dans l'espace documentaire auquel l'utilisateur pourra se référer et dans lequel les principales évolutions à jour seront communiquées.

1.1 Respect des lois en vigueur

Dans le cadre de l'usage des **moyens de communication électronique** mis à sa disposition par la **Collectivité**, l'**utilisateur** est tenu au respect de la présente Charte, mais également au respect des dispositions législatives et réglementaires en vigueur.

L'**utilisateur** doit notamment respecter :

1- la réglementation relative aux libertés individuelles et les règles d'ordre public ;
2- la réglementation relative aux droits de propriétés intellectuelles, qui interdisent notamment de reproduire et de diffuser les logiciels sans autorisation, pour quelque usage que ce soit. Il en est de même d'une part, pour toutes œuvres telles que photographies, images, bases de données, œuvres audiovisuelles ou musicales, textes, etc. protégées par le droit d'auteur, et d'autre part, pour les marques, dessins et modèles, noms de domaine et autres signes distinctifs, en l'absence d'autorisation expresse, leur exploitation étant interdite ;
3- la réglementation relative à la protection des données à caractère personnel (cf. chapitre 4).

4- la réglementation relative à la fraude informatique, qu'il s'agisse de l'intrusion dans un système de traitement automatisé de données, du maintien ou de l'altération des éléments qu'il contient, étant précisé que ces actes sont passibles de sanctions pénales.

1.2 Objet de la Charte

La présente Charte a pour objet de préciser les responsabilités des **utilisateurs** en accord avec la législation, afin de garantir la sécurité et le bon fonctionnement du **système d'information**.

La Charte définit les conditions générales d'utilisation des **moyens de communication électronique**, ressources informatiques, téléphoniques, informationnelles, numériques et technologiques de la **Collectivité** en
précisant le cadre légal.

La Charte précise les conditions et les limites des éventuels contrôles portant sur l'utilisation de ces ressources.

Elle précise enfin les sanctions applicables en cas de contravention aux règles établies ou rappelées par la Charte.

Ce document annule et remplace tous les précédents documents de même nature émis par la Région Hauts-de-France, les ex-Régions Nord - Pas de Calais et Picardie relatifs à l'utilisation du **système d'information**.

1.3 Définitions

Les termes ci-dessous, qu'ils soient écrits au singulier ou au pluriel, reçoivent la définition et la signification suivantes :

- ***Administrateur fonctionnel*** : Désigne la ou les personne(s) en charge de gérer les systèmes informatiques, d'établir les paramétrages, la gestion des droits et les accès sur un périmètre défini du système d'information.
- ***Administrateur technique*** : Désigne la ou les personne(s) en charge d'installer, de gérer l'infrastructure informatique et téléphonique. Il assure ainsi le maintien en condition opérationnelle du système d'information. Un administrateur technique est souvent également administrateur fonctionnel.

Lorsque le terme **administrateur** est employé seul, il identifie l'une et l'autre de ces définitions.

- ***Collectivité*** : La personne morale Région Hauts-de-France qui fournit les ressources informatiques, téléphoniques, informationnelles, numériques et technologiques et les met à disposition du personnel.
- ***Délégué à la protection des données*** : Personne désignée par le Président du Conseil régional, qui a pour mission de veiller à la bonne application au sein de la **Collectivité** du Règlement Général sur la Protection des Données (RGPD 2016/679 EU) et la loi du 6 janvier 1978 modifié en 2004 relative à l'informatique, aux fichiers et aux libertés. Le délégué à la protection des données remplace le correspondant informatique et libertés conformément au RGPD.
- ***Moyens de communication électronique*** : Outils et services mis à la disposition des utilisateurs du système d'information pour communiquer. Il s'agit des outils et services de messagerie électronique, des outils et services d'accès aux réseaux informatiques internes et externes, des outils et services de téléphonie.

- ***Poste de travail*** : Ensemble des équipements matériels, logiciels et services mis à la disposition des utilisateurs pour leur permettre d'assurer leurs missions et d'accéder aux moyens de communication électronique.
- ***Responsable hiérarchique*** : Désigne les personnes qui ont autorité sur les agents placés sous leur responsabilité et dont ils ont ordonné les missions (directeur général, directeur, responsable de département, responsable de service et de secteur). La notion s'entend par extension à la chaine hiérarchique complète (n+1, n+2…).
- ***Responsable informatique*** : Désigne la personne en charge de l'organisation et du management des outils et services informatiques et numériques, support du Système d'information de la Région Hauts-de-France. Il est le garant du maintien en condition opérationnelle du Système d'information.
- ***Responsable de la sécurité du système d'information*** : Désigne la personne en charge de l'organisation et du management de la sécurité du système d'information de la Région Hauts-de-France.
- ***Système d'Information*** : Ensemble de tous les éléments qui contribuent au traitement et à la circulation de l'information dans la **Collectivité** (base de données, logiciels d'application, procédures, …) et du système informatique (serveur, périphériques, imprimantes, copieurs multifonction, système d'exploitation, …).
- ***Utilisateurs*** : les personnes visées à l'article 2 de la présente Charte.
- ***Visiteurs*** : les personnes, sans lien contractuel avec la **Collectivité**, reçues dans ses locaux.

2 CHAMP D'APPLICATION

Les dispositions de la présente Charte s'appliquent aux personnes autorisées à accéder aux ressources informatiques, informationnelles, numériques et technologiques et à utiliser les **moyens de communication électronique** de la **Collectivité** :

- les agents régionaux titulaires et non titulaires ;
- les apprentis ;
- les stagiaires ;
- les intervenants extérieurs, prestataires ;
- les visiteurs.

3 OPPOSABILITÉ DE LA CHARTE

La présente Charte est portée à la connaissance des **utilisateurs** par tous moyens jugés adéquats par la **Collectivité**. Constitue notamment un moyen adéquat et suffisant l'un des moyens suivants : diffusion sur l'intranet, annexe signée aux conventions de stage pour les stagiaires externes, transmission individuelle via la messagerie électronique pour les **utilisateurs**.

4 PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Le Règlement Général sur la Protection des Données (RGPD 2016/679 UE) et la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ont pour objet de protéger les personnes contre les dangers d'une utilisation abusive de fichiers contenant des données à

caractère personnel. Ils définissent les conditions dans lesquelles des données à caractère personnel peuvent être recueillies et faire l'objet d'un traitement. Ils ouvrent aux personnes concernées par les traitements un droit d'accès et de rectification de leurs données enregistrées. Les atteintes aux droits des personnes concernées par les traitements de données à caractère personnel sont pénalement répréhensibles.

Conformément à la législation, la **Collectivité** désigne son **délégué à la protection des données à caractère personnel.** Les **utilisateurs** qui souhaitent réaliser des traitements de données à caractère personnel doivent impérativement et obligatoirement consulter le **délégué** préalablement à la mise en œuvre du traitement. Ce dernier recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de la **Collectivité** au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande.

Le **délégué** veille au respect des droits des personnes (droit d'accès, de rectification et d'opposition). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le **délégué**.

5 SÉCURITÉ

La **Collectivité** met en œuvre les mesures humaines, organisationnelles et techniques appropriées pour assurer la sécurité matérielle et logicielle du système d'information et de communication.

L'**utilisateur** est acteur de la sécurité du **système d'information**. Il est responsable de l'usage qu'il fait des ressources informatiques et des réseaux auxquels il a accès. Il a le devoir de s'informer des règles de sécurité générales et propres aux systèmes d'information auprès du **responsable informatique** et dans les espaces documentaires mis à sa disposition. À son niveau, il a aussi, la charge de contribuer à la sécurité générale en respectant les règles d'utilisation, de sécurité et de bon usage. L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement.

L'**utilisateur** doit rester vigilant et est tenu d'avertir le **responsable informatique** de :

- toute violation ou tentative de violation suspectée de ses accès ;
- de toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation ;
- de toute constatation d'un fonctionnement inhabituel ou anormal ;
- de toutes anomalies découvertes (intrusion dans le réseau, vol/perte de matériel, etc.) ;
- et de manière générale, de tout comportement anormal du poste de travail.

Il signale au **délégué à la protection des données** de la **Collectivité** toute atteinte aux données à caractère personnel qu'il peut constater.

En fonction du niveau de l'incident, le **responsable informatique** informera le **responsable de la sécurité du système d'information**.

6 USAGE DES RESSOURCES INFORMATIQUES, INFORMATIONNELLES, NUMÉRIQUES ET TECHNOLOGIQUES

6.1 Principe d'usage professionnel

Les **moyens de communication électronique** de la **Collectivité** sont mis à la disposition des **utilisateurs** à des fins professionnelles dans le cadre de leurs attributions et fonction. Il en résulte qu'un usage personnel de ces moyens est une simple tolérance de la part de la **Collectivité**, il doit être raisonnable, à caractère exceptionnel et s'inscrire dans le cadre des nécessités de la vie courante et familiale, ne pas affecter le bon fonctionnement du **système d'information** et doit être conforme aux conditions précisées dans la présente Charte.

L'utilisation des **moyens de communication électronique** doit respecter a minima les règles essentielles énoncées dans la présente Charte, l'**utilisateur** est tenu notamment de :

- utiliser ces moyens conformément aux lois et aux règlements, à l'ordre public et aux bonnes mœurs, au respect de l'image de la **Collectivité** ;
- respecter les notes techniques et de service, principes d'utilisation, procédures relatives à leur mise en œuvre qui constituent des documents associés à la Charte. Ces derniers sont mis à disposition dans les espaces documentaires ;
- respecter la confidentialité des données échangées et traitées.

Il convient de rappeler que les **visiteurs** ne peuvent pas avoir accès au **système d'information** de la **Collectivité mais seulement à Internet via le réseau Wifi dédié aux visiteurs après avoir décliné son identité auprès de la personne habilitée par la DSI à fournir un code d'accès à la connexion.**

Seule la DSI est habilitée à fournir des accès aux systèmes d'information aux prestataires de service.

Les intervenants extérieurs doivent s'engager à faire respecter la présente Charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre la **Collectivité** et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

L'**utilisateur** est responsable de l'usage qu'il fait des **moyens de communication électronique** mis à sa disposition par la **Collectivité**. Lorsque l'**utilisateur** en fait un usage personnel, il en assume la pleine et entière responsabilité et toutes les conséquences juridiques.

6.2 Télétravail, travail en mobilité et usage de matériel non professionnel

6.2.1 Télétravail

L'agent exerçant son activité selon les modalités propres au télétravail s'engage à respecter la présente Charte aussi bien dans les locaux de la **Collectivité** que sur son lieu de télétravail.

Il est rappelé que les tiers lieux autres que les locaux sous le contrôle direct de la **Collectivité** peuvent porter des risques spécifiques auxquels l'**utilisateur** doit apporter une attention particulière (perte, vol, confidentialité des données et des traitements – dont impression…).

. L'**utilisateur** doit respecter les recommandations suivantes :

- Sécurisez votre connexion WiFi à votre domicile (utilisez un mot de passe long et complexe), suivez les instructions de mise à jour de votre fournisseur d'accès internet.
- Tout usage de l'équipement nécessite l'usage du client VPN fourni par la DSI

- Séparer vos usages professionnels et personnels au risque de les confondre et de générer des fautes de sécurité. L'activité professionnelle doit se faire sur vos moyens professionnels et seulement sur vos moyens professionnels.

Les principes de sécurité énoncés aux 10.2 « Sécurité » & 10.3 « Pérennité des données » s'appliquent également dans ces cas de figure.

6.2.2 Travail en mobilité

Le travail en mobilité – dans les transports en commun, chez les partenaires, etc. – augmente sensiblement les risques de sécurité liés au **système d'information**. Dans ces situations, l'**utilisateur** doit être encore plus attentif aux problématiques de confidentialité d'accès aux informations et à la protection de l'intégrité des équipements qui lui sont confiés.

La connexion des matériels à des réseaux informatiques autres que ceux de la **Collectivité** est tolérée, sous réserve que l'**utilisateur** prenne préalablement toute disposition afin de s'assurer des bonnes pratiques de sécurité et, le cas échéant, de veiller au respect des chartes qui pourraient s'appliquer localement. Il est rappelé que les réseaux ouverts tels que les wifi « gratuits » dans les lieux publics ou partagés (hôtels) représentent un risque important de compromission des communications. Il convient d'en limiter l'usage aux cas d'impérative nécessité.

Pour renforcer la sécurité, l'**utilisateur** s'appuiera sur les dispositifs matériels ou logiciels de sécurité (antivirus, chiffrement, filtre de confidentialité, connexion VPN…) mis à disposition par la **Collectivité** et les bonnes pratiques diffusés dans l'espace documentaire dédié

L'usage des supports externes (Clé USB, disque externe…), est interdit.. L'**utilisateur** doit en particulier vérifier l'innocuité du dispositif avant son utilisation.

6.2.3 Usage de matériel non professionnel

La connexion aux réseaux de la **Collectivité** (wifi, Bluetooth, filaire…) de matériel qui n'a pas été fourni ou contrôlé par le **responsable informatique** est strictement interdite.

L'accès à la messagerie professionnelle depuis un matériel personnel (ordinateur, téléphone multifonction, tablette…) est toléré à la condition expresse que l'**utilisateur** ait mis en œuvre sur les dits matériels les mesures de sécurité adaptées. Par exemple – liste non exhaustive, obligation d'un code d'accès, antivirus activés, protection du dispositif contre les attaques en brute de force, chiffrement local…

L'accès aux ressources de l'intranet depuis l'extérieur du réseau (mode extranet) est toléré dans les mêmes conditions que celles du paragraphe précédent.

6.3 Gestion des accès

Sous la responsabilité et le contrôle de la **Collectivité**, le **responsable informatique** délivre les moyens d'authentification propres à chaque **utilisateur** (code confidentiel, carte à puce…) pour lui permettre l'accès aux **moyens de communication électronique**.

Pour tous les systèmes d'authentification, l'**utilisateur** doit respecter les règles de délivrance et de mise à jour en vigueur dans la **Collectivité**.

Les moyens d'authentification sont personnels, confidentiels et non transmissibles.

Toutes les connexions réalisées à l'aide de ces authentifiants, en particulier pour une utilisation malveillante, engagent la responsabilité de son propriétaire. En conséquence de quoi, il convient de respecter les règles de sécurité suivantes :

- ne pas les inscrire sur support papier ou électronique à proximité des outils informatiques mis à disposition ou sur ceux-ci, ainsi que de les stocker en clair dans un registre, un programme ou un fichier ;
- ne jamais confier son identifiant/mot de passe, même à son **responsable hiérarchique** ;
- ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur ;
- ne pas utiliser ou essayer d'utiliser les moyens d'authentification autres que les siens et/ou masquer sa véritable identité.

Par ailleurs, l'**utilisateur** doit également veiller à toujours bloquer l'accès à son **poste de travail**, dès qu'il s'en éloigne, même pour quelques instants.

L'accès aux **moyens de communication électronique** sera supprimé lors de la cessation définitive de l'activité professionnelle (retraite, mutation, départ, etc.). Toutefois cet accès pourra être maintenu temporairement par le **responsable informatique** après autorisation du **responsable hiérarchique**. L'agent devra faire au préalable une demande expresse de maintien temporaire d'accès aux données pour une durée précise qui ne pourra être supérieure à 3 mois. L'accès pourra être suspendu dès lors qu'un usage illicite ou abusif sera suspecté ou démontré.

Sur la validation expresse du **responsable hiérarchique** et lorsque les informations détenues sont nécessaires à la poursuite de l'activité de la **Collectivité**, le **responsable informatique** pourra transférer les droits d'accès sur une application informatique, un poste de travail, un espace de stockage d'un **utilisateur** vers un autre **utilisateur** désigné par le **responsable hiérarchique**. L'**utilisateur** en sera informé, par tous les moyens possibles.

7 MESSAGERIE ÉLECTRONIQUE

L'utilisation des systèmes de courriers électroniques basés sur l'internet, autres que ceux mis à disposition par la **Collectivité**, est tolérée à partir du poste de travail dans les mêmes conditions que celles décrites dans l'article 6.1.

La **Collectivité** met à disposition une boite aux lettres électroniques nominative. L'utilisation de cette adresse nominative est de la responsabilité de l'**utilisateur**. L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative. Il ne retire en rien le caractère professionnel de la messagerie

Par exception au principe d'utilisation à des fins professionnelles, il est toléré un usage à titre privé de la messagerie mise à disposition par la **Collectivité**, sous réserve que cet usage soit raisonnable, à caractère exceptionnel, strictement inscrit dans le cadre des nécessités de la vie courante et familiale et conforme aux conditions précisées dans la présente Charte. En particulier, cet usage doit être limité en volume et en durée de façon à ne pas affecter le bon fonctionnement du **système d'information** de la Collectivité. Dans ce contexte, l'**utilisateur** est tenu de marquer les messages qu'il reçoit et/ou envoie dans le champ « objet » avec la mention ***[PERSONNEL]*** et, le cas échéant, à les stocker dans un dossier spécifique dénommé « ***Personnel*** ».

En cas d'usage privé abusif avéré de la messagerie (fréquence des messages reçus ou envoyés, volume des données échangées, type/taille/format des pièces jointes, nombre de destinataire, etc.) ou, en cas d'utilisation abusive ou malveillante avérée de la mention ***[PERSONNEL]*** la **Collectivité** sera en droit d'en tirer toutes les conséquences sur le plan juridique, judiciaire et disciplinaire, le cas échéant.

En cas d'absence et de nécessité de service , le supérieur hiérarchique est autorisé à consulter les mails de ses dossiers, exception faite du dossier nommé « Personnel ».

Une adresse électronique fonctionnelle ou organisationnelle peut être mise en place pour un **utilisateur** ou un groupe d'utilisateurs.

La messagerie électronique est mise à la disposition des **utilisateurs** à des fins professionnelles. Les échanges réalisés par ce biais pouvant engager la responsabilité de la **Collectivité**, l'**utilisateur** est tenu de respecter les procédures habituelles de relecture et de validation qui sont applicables aux correspondances internes et externes.

Il est interdit à l'**utilisateur** d'envoyer des messages en « masse » et de répondre à des « chaînes » de messages – du type messages à vocation charitable ou qui laissent entrevoir des améliorations financières ou autres.

Seront considérés comme fautifs ou abusifs les comportements suivants :

- tout message contraire à la réglementation en vigueur et aux bonnes mœurs tels que les messages à caractère xénophobe, raciste, négationniste, pédopornographique, faisant l'apologie du terrorisme ou de prosélytisme religieux ;
- l'échange de messages à caractère, pornographique mais aussi ceux contribuant à un harcèlement sexuel ou moral, de menaces ou d'insultes ;
- l'échange d'informations confidentielles au mépris des dispositions internes relatives à la confidentialité des échanges et du secret professionnel ;
- la redirection de sa messagerie vers une messagerie externe à la **Collectivité**.

D'une manière générale, l'utilisation de la messagerie ne doit pas porter atteinte à l'image, à la réputation, à la sécurité d'autrui ou de la **Collectivité** ainsi qu'au bon fonctionnement du **système d'information** de la **Collectivité**.

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes (cf. chapitre 11, page 13).

L'**utilisateur** veille à la pertinence du choix des destinataires.

L'**utilisateur** est tenu de ne pas ouvrir les messages ainsi que les fichiers attachés aux messages pour lesquels il a des doutes sur l'émetteur et/ou le contenu.

Afin d'assurer la continuité de service, le **responsable hiérarchique** doit, dans la mesure du possible, anticiper les incidences des absences ou mobilités des agents. Avant l'échéance, il doit s'assurer que le transfert des données et des droits d'accès ont été effectués et que les interlocuteurs des agents ont été correctement informés (par exemple par un message automatique d'absence ou des délégations de droits).

L'**utilisateur** est informé que des dispositifs et procédures de contrôle pourront être mis en place par la **Collectivité** et s'appliquer à tous les messages émis et reçus sans distinction.

8 INTERNET

L'accès à internet est attribué par le **responsable informatique** de la **Collectivité**.

L'**utilisateur** est tenu de consulter les sites internet à des fins professionnelles. La consultation des sites internet à des fins personnelles est une simple tolérance, ayant un caractère nécessairement exceptionnel, et sous réserve que cette consultation ne perturbe pas le bon fonctionnement du service et reste en dehors du temps de travail, et que la durée et le volume de connexion restent raisonnables.

La consultation doit se limiter à des sites internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs. Il est notamment interdit :

- de rechercher, visualiser télécharger, transmettre ou conserver des contenus à caractère pornographique, pédophile, raciste, xénophobe, diffamatoire, discriminatoire, portant atteinte au respect de la personne humaine et à sa dignité, incitant à la commission d'un délit ou d'un crime, contraire à l'ordre public ou aux bonnes mœurs, attentatoires à l'image interne ou externe de la **Collectivité** ;
- de consulter des sites susceptibles de comporter un risque pour le **système d'information** de la **Collectivité**, encombrer ou saturer le réseau, permettant de contourner les dispositifs de protection technique ou de porter atteinte à la confidentialité des informations ;
- de créer ou de mettre à jour, au moyen de l'accès à l'internet qui est fourni par la **Collectivité**,

tout site internet (notamment, page personnelle, journal personnel en ligne, etc.) en dehors du cadre strictement professionnel et dûment autorisé.

De manière générale, l'utilisation des services Internet à des fins mercantiles ou illicites est interdite.

En cas d'abus, pour des raisons de sauvegarde et de sécurité du **système d'information**, le **responsable informatique** aura la faculté de faire supprimer ou de restreindre ponctuellement la connexion à internet.

L'**utilisateur** est informé que des dispositifs et procédures de contrôle sont mis en place par la **Collectivité** et s'appliquent à l'ensemble de la navigation sur l'internet.

L'**utilisateur** est informé des risques liés à l'utilisation des modes de communication sur les forums en ligne, réseaux sociaux ou sites collaboratifs au regard de la responsabilité de l'**utilisateur**, vis-à-vis de la **Collectivité** et des tiers, sur les propos émis.

Dans le cadre de ce type de participation, l'**utilisateur** est tenu de respecter l'ensemble des règles de la présente Charte, et en particulier au titre de la confidentialité : le respect de l'obligation de réserve et du secret professionnel.

L'**utilisateur** doit veiller de ne pas encombrer, engorger ou ralentir les accès aux réseaux lorsqu'il accède à des médias en temps réel, musique ou vidéo en ligne, téléchargement de fichiers.

Il en résulte que l'**utilisateur** se doit de réserver l'utilisation de ces modes de communication dans le cadre de la stricte nécessité de ses fonctions au sein de la **Collectivité**.

8.1 Réseaux sociaux

8.1.1 Usage professionnel

Un **utilisateur** peut être amené dans le cadre de ses missions à animer des réseaux sociaux au nom de la **Collectivité**. L'usage de réseaux sociaux professionnels est autorisé par le **responsable hiérarchique**, seul compétent pour en déterminer les conditions d'utilisation.

De plus, si l'autorisation a été donnée, **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 la **Collectivité** ;
- répondre aux contributions des tiers avec pertinence, exactitude, en s'efforçant de ne pas porter atteinte à l'image de la **Collectivité** ;
- respecter les conditions générales d'utilisation du réseau social et l'ensemble des lois applicables ;
- utiliser uniquement les outils de communication de la **Collectivité**, selon les instructions qui lui ont été données et valoriser la visibilité du site web de la **Collectivité** ;
- s'abstenir de diffuser toute information confidentielle ou toute information sensible relative à la **Collectivité**.

En cas de doute sur l'utilisation d'un réseau social, l'**utilisateur** devra immédiatement consulter son **responsable hiérarchique**.

L'autorisation donnée pourra être retirée, modifiée ou suspendue par le **responsable hiérarchique**.

L'**utilisateur** devra prendre toutes les précautions utiles pour que son utilisation des réseaux sociaux soit sans danger pour les **systèmes d'information** de la **Collectivité**.

8.1.2 Usage personnel

Il est interdit à l'**utilisateur** de porter atteinte à ses devoirs de neutralité et de discrétion professionnelle et de communiquer notamment des informations confidentielles, des informations sensibles relatives à la **Collectivité** ou des informations couvertes par un secret légalement protégé.

Les catégories proposant, à la fois, des contenus à caractère professionnel et personnel tels que les réseaux sociaux et les forums sont autorisées dans la limite d'un usage raisonnable et à condition de ne pas mettre en cause l'intérêt, l'image ou la réputation de la **Collectivité**.

L'**utilisateur** n'est autorisé à faire mention de son appartenance à la **Collectivité** que dans la mesure où cette divulgation ne porte pas atteinte à ses obligations de discrétion et de neutralité, ni à l'image ou à la réputation de la **Collectivité**.

8.2 Service dans le nuage (cloud)

L'informatique dans le nuage est un concept qui consiste à déporter sur des serveurs distants des stockages et des traitements informatiques traditionnellement localisés sur des serveurs locaux ou sur le poste de l'**utilisateur**.

Les services dans le nuage portent un risque pour la **Collectivité** de la perte de souveraineté et de contrôle sur les données qu'elle produit (disponibilité, confidentialité…).Leur usage est strictement interdit

9 TÉLÉPHONIE

L'**utilisateur** est tenu d'utiliser les outils de téléphonie (téléphone fixe, mobile, télécopie, téléphone multifonction et tout autre moyen de téléphonie) mis à sa disposition par la **Collectivité** à des fins professionnelles, et conformément aux lois et règlements, à l'ordre public et aux bonnes mœurs, au respect de l'image de la **Collectivité**.

Par exception au caractère exclusivement professionnel, il est toléré un usage raisonnable, à caractère exceptionnel, à titre privé, de ces outils de téléphonie, dans le cadre des nécessités de la vie courante et familiale et conformément aux prescriptions de la présente Charte.

L'**utilisateur** est informé que la **Collectivité** pourra mettre en place des dispositifs techniques permettant notamment de contrôler le coût et le nombre d'appels téléphoniques, SMS, consommation multimédia et internet.

10 POSTES DE TRAVAIL ET DISPOSITIFS MOBILES

10.1 Propriété des matériels et des logiciels

Les matériels et logiciels sont mis à disposition par le **responsable informatique** en fonction des besoins et impératifs des missions. Ils demeurent la propriété de la **Collectivité**. L'**utilisateur** est et demeure responsable des matériels et logiciels qui lui sont confiés, il doit en prendre soin. Ils sont restitués obligatoirement à la DSI selon les procédures en vigueur en cas de mobilité interne ou avant le départ définitif.

En prévision d'une cessation d'activité ou d'une mobilité et sous-couvert de son **responsable hiérarchique**, l'**utilisateur** s'assurera que ses données sont sauvegardées (disques partagés, boite de messagerie, espaces collaboratifs…) et que les droits d'accès sont transférés à/aux **utilisateurs** désignés par le **responsable hiérarchique**. Pour les données à caractère privé, elles auront été supprimées.

10.2 Sécurité

10.2.1 Principes généraux

Des perturbations au fonctionnement du **système d'information** de la **Collectivité**, peuvent être générées du fait de l'ajout, la suppression d'équipements matériels ou logiciels ou en raison de la modification des données nécessaires à son fonctionnement. En conséquence, l'**utilisateur** ne doit pas modifier la configuration matérielle ou logicielle de son **poste de travail** ou des dispositifs mobiles. Seule la DSI est habilitée à acheter, installer, configurer ou supprimer les logiciels du poste de travailDe même, l'**utilisateur** est tenu à ne pas connecter de modem ou périphérique de communication sur son **poste de travail** ou dispositif mobile, ni à y installer de logiciel ou de matériel, sans l'autorisation expresse du **responsable informatique**. L'usage de la fonctionnalité « partage de connexion » d'un téléphone professionnel vers un équipement professionnel est autorisé.

10.2.2 Perte ou vol d'un équipement professionnel

Tous les dispositifs mobiles doivent être rangés dans un endroit sécurisé. Lors de déplacements, l'**utilisateur** doit veiller à ne pas les laisser apparents dans un véhicule, ou tout autre lieu.

En cas de perte ou de vol du dispositif mobile confié, l'**utilisateur** doit effectuer une déclaration auprès du commissariat de police le plus proche, et ce dans les plus brefs délais et adresser une copie aux services concernées (juridique, finance, informatique…) selon la procédure interne. Une copie de cette déclaration est à adresser au **responsable de la sécurité du système d'information**.

L'utilisateur en informe immédiatement le **responsable informatique** afin que celui-ci fasse appliquer les précautions adaptées à l'incident de sécurité (verrouillage de compte, droits d'accès, supervision active, surveillance renforcée…).

Toute déclaration volontairement fausse est passible de sanctions disciplinaires et/ou pénales.

10.3 Pérennité des données

Conformément aux obligations réglementaires et aux procédures internes d'archivage électronique, l'**utilisateur** ne doit détruire les fichiers ou les documents sur lesquels sa fonction et ses missions le conduisent à intervenir qu'après s'être assuré que cette destruction ne porte aucun préjudice à la **Collectivité**.

Les données professionnelles doivent être obligatoirement enregistrées sur les serveurs professionnels et non en local sur l'équipement fourni.

11 CONFIDENTIALITÉ

L'**utilisateur** a une obligation générale et permanente de confidentialité et de discrétion attachée à l'utilisation des informations et documents électroniques exploités dans le cadre de ses missions au sein de la **Collectivité**.

En tout état de cause, les obligations administratives inhérentes au devoir de réserve et au respect du secret professionnel s'appliquent à l'utilisation des **moyens de communication électronique** qui sont mis à disposition de l'**utilisateur** par la **Collectivité**.

Toute copie de données professionnelles sur un support externe est interdite.

11.1 Stockage des données

L'utilisateur doit obligatoirement stocker ses données professionnelles sur les serveurs professionnels (stockage interdit sur clé USB, disque dur externe, équipement personnel). Pour transférer des données volumineuses vers l'extérieur, le service «depot.hautsdefrance.fr » est à disposition.

En cas de non-respect de l'une de ces dispositions, les fichiers stockés seront susceptibles d'être effacés par **la DSI** et son **utilisateur** en sera informé.

12 CONTRÔLE – TRAÇABILITÉ – CONSERVATION

Dans le respect des principes de transparence et de proportionnalité, des exigences légales et réglementaires, à des fins de sécurité et de vérification du bon accès et usage des **moyens de communication électronique**, ainsi que du bon fonctionnement du **système d'information**, des systèmes de filtrage, de contrôle et des dispositifs d'enregistrement des traces d'activité des systèmes peuvent être mis en place par le **responsable informatique**. Le fonctionnement des systèmes de contrôle, de filtrage et d'enregistrement de trace des activités des systèmes est assuré par les **administrateurs techniques** en fonction de leur domaine de compétences. Ceux-ci appliquent la Politique de Sécurité des Systèmes d'Information définie et validée par la **Collectivité**.

Les systèmes de contrôle sont mis en œuvre pour contrôler les messages entrant et sortant et également pour bloquer, notamment sur la base d'une liste de mots clefs, de type de fichiers joints ou de tailles des messages, les échanges informatiques.

Les systèmes de filtrage sont mis en œuvre pour contrôler les flux de communication Internet et également pour bloquer, notamment sur la base de listes de catégories et de mots clefs, l'accès aux contenus externes au réseau de la **Collectivité**.

Les systèmes de restriction d'usage sont mis en œuvre pour limiter ou interdire certains services accessibles depuis les téléphones fixes et mobiles pour ceux qui en sont dotés.

L'**utilisateur** est informé que, *a minima,* les traces suivantes sont conservées :

- liste des contenus ou services auxquels l'**utilisateur** a eu accès sur le réseau Internet, intranet, extranet ;
- date et heure des connexions ou tentatives de connexion de l'**utilisateur** sur les systèmes d'accès aux **moyens de communication électronique** ;
- liste des paramètres techniques de gestion des services de messagerie électronique (identification du compte **utilisateur**, coordonnées du destinataire, date et heure, etc.) ;
- liste des traces de connexion aux applications et aux ressources informatiques.

Les traces, messages et documents pourront être conservés pour une durée maximale d'un an, sous réserve du respect des dispositions légales et réglementaires applicables au titre de la prescription.

À des fins statistiques relatives aux connexions et aux contacts réalisés, des contrôles portant sur la volumétrie des connexions à des sites Internet ou de l'utilisation de la messagerie pourront être réalisés par le **responsable informatique**.

L'**utilisateur** est informé que des contrôles individualisés pourront être diligentés par le **responsable de la sécurité du système d'information** à la suite d' un dysfonctionnement du **système d'information**, d'une alerte de sécurité et également en cas de suspicion d'un usage non conforme des **moyens de**

communication électronique, sous réserve du respect des dispositions applicables au secret des correspondances privées.

13 ADMINISTRATEUR TECHNIQUE OU FONCTIONNEL

13.1 Missions et rôle de l'administrateur

L'**administrateur** est garant du bon fonctionnement et de la sécurité des **moyens de communication électronique** ainsi que de la disponibilité des données et des applications informatiques de la **Collectivité**.

Dans l'exercice de ces missions, l'**administrateur** veille à faire respecter les droits et devoirs des **utilisateurs** qui sont définis par la présente Charte et en application des dispositions légales et réglementaires.

13.2 Droits de l'administrateur fonctionnel

Les **utilisateurs** sont informés que l'**administrateur fonctionnel** peut avoir accès aux **systèmes d'Information** couverts par son domaine de compétence, à n'importe quel moment et ce afin d'effectuer tout acte de gestion, ce qui comprend notamment :

- le paramétrage fonctionnel ;
- la gestion des habilitations et des droits d'accès ;
- la protection de l'intégrité et de la confidentialité des données et du fonctionnement du **système d'information** couvert.

13.3 Droits de l'administrateur technique

Les **utilisateurs** sont informés que l'**administrateur technique** peut avoir accès à l'ensemble du **système d'information** de la **Collectivité**, à n'importe quel moment et ce afin d'effectuer tout acte de protection, ce qui comprend notamment :

- la sauvegarde, la conservation et la diffusion des informations collectées et traitées dans le cadre des activités de la **Collectivité** ;
- la preuve de la date de création ou de la diffusion desdites informations ;
- l'absence d'intrusion dans le **système d'information** ou de matériels en violation des dispositions légales et réglementaires en vigueur ;
- la mise à jour, la maintenance, la correction et la réparation des matériels et logiciels nécessaires à l'utilisation du **système d'information**.

À cette fin, l'**administrateur technique** est habilité à mettre en place des outils de contrôle et de surveillance, à examiner des fichiers, des messages électroniques ou des relevés de communication, répondant à la finalité de sécurité du **système d'information** de la **Collectivité** et à l'application de la présente Charte.

13.4 Devoirs de l'administrateur

L'**administrateur** est tenu à une obligation de confidentialité stricte. Sauf dans les cas où sa responsabilité pénale est susceptible d'être engagée et également dans les cas où la sécurité ou le bon fonctionnement du **système d'information** sont menacés ainsi que l'intérêt de la **Collectivité**,

l'**administrateur** ne doit pas utiliser ou divulguer les informations couvertes par le secret professionnel ou le secret des correspondances privées, et, de façon plus générale toutes les informations relatives à la vie privée des **utilisateurs**.

Les **administrateurs** sont autorisés à prendre la main à distance sur les **postes de travail** des **utilisateurs** afin de résoudre les problèmes signalés.

Durant les heures ouvrées, la prise de main devra être réalisée avec l'accord préalable de l'**utilisateur**. Dans le cadre de mises jour et évolutions du **système d'information**, et lorsqu'aucun **utilisateur** n'est connecté sur son **poste de travail**, l'**administrateur** peut être amené à intervenir sur l'environnement technique des **postes de travail**. Il s'interdit d'accéder aux contenus.

Par exception, en cas de situation grave, et notamment en cas d'attaque virale, la prise de main à distance par l'**administrateur technique** pourra être réalisée sur tous les postes jugés suspects. Toutefois, cette prise de main sans autorisation ne sera légitime que dans les cas où ces postes de travail présentent un danger pour le **système d'information** de la **Collectivité**. En tout état de cause, l'**administrateur** est tenu d'en informer préalablement le **responsable informatique** et le **responsable de la sécurité du système d'information**.

Les **administrateurs** ont l'obligation d'informer immédiatement les **utilisateurs** et leur **responsable hiérarchique** des violations constatées aux règles de la présente Charte. Ils assurent la traçabilité de l'incident et des actions menées.

Seul l'**administrateur technique** est autorisé à introduire dans le **système d'information** de nouveaux matériels ou logiciels. Il en résulte que l'**utilisateur** est tenu d'informer l'**administrateur technique** de ses besoins en matériel et/ou logiciels nouveaux, en rapport avec le **poste de travail** et la mission confiée à l'agent, suffisamment longtemps à l'avance pour que l'**administrateur technique** ait le temps de déterminer les impacts possibles de ces ajouts sur le **système d'information**. L'**administrateur technique** s'engage à mettre tout en œuvre pour intégrer le nouveau composant, étant précisé qu'il est habilité à refuser ledit composant en raison notamment des risques pour le **système d'information**. Ce refus est motivé.

14 SANCTIONS

Tout usage détourné, fautif ou abusif des **moyens de communication électronique** et du système d'information mis à disposition par la **Collectivité** est susceptible d'être sanctionné.

Conformément à la réglementation, la **Collectivité** se réserve le droit de saisir le Procureur de la République et notamment dans l'hypothèse où il serait contrevenu à une des règles précitées. Le **responsable informatique** doit saisir sa hiérarchie.

En cas de non-respect des dispositions de la présente Charte et pour préserver le bon fonctionnement du **système d'information** de la **Collectivité**, l'**utilisateur** peut se voir appliquer les sanctions suivantes :

- suspension, restriction ou suppression de l'accès aux ressources informatiques, informationnelles, numériques ou technologiques ;

- isolement, neutralisation ou effacement de toute donnée ou fichier manifestement en contradiction avec la Charte ou qui mettrait en péril la sécurité du **système d'information** ;
- déconnexion d'un **utilisateur** ou retrait des moyens mis à disposition, avec ou sans préavis dans le respect du droit applicable en matière disciplinaire.

Dans un premier temps, les droits d'accès pourront être suspendus temporairement sans délai par le **responsable informatique**. L'utilisateur en sera informé.

Dans un second temps, tout manquement grave ou récidive, qualifié par le **responsable de la sécurité du système d'information**, pourra faire l'objet d'une notification à sa hiérarchie et aux autorités de contrôle interne. Il pourra être passible de poursuites civiles ou pénales sans préjuger d'éventuelles sanctions disciplinaires proportionnelles aux manquements constatés, comme prévues dans le statut de la fonction publique territoriale.

En cas de pertes ou de détériorations répétées des matériels confiés, des sanctions pourront également être appliquées.

La Collectivité se réserve le droit de demander à l'**utilisateur** le remboursement des frais engendrés par l'exploitation d'un service non prévu dans la dotation de l'**utilisateur** – par exemple, dans un forfait téléphonique fourni à titre professionnel.

15 SPÉCIFICITÉS APPLICABLES AUX REPRÉSENTANTS DU PERSONNEL, DÉLÉGUÉS SYNDICAUX ET ORGANISATIONS SYNDICALES

Il est rappelé que les représentants du personnel et les représentants syndicaux utilisent dans le cadre de leur mandat, les outils de communication électronique qui leur sont attribués pour l'exercice de leur activité professionnelle. Le protocole d'accord relatif à l'exercice des droits et moyens syndicaux précise les conditions d'utilisation des outils de communication électronique et du système d'information.

Les organisations syndicales ont la possibilité de contacter les agents individuellement par messagerie électronique. Il est rappelé une obligation de confidentialité à laquelle la **Collectivité** et organisations syndicales sont tenues. La confidentialité des échanges électroniques entre le personnel, les représentants syndicaux et les organisations syndicales est garantie.

La **Collectivité** s'engage à n'exercer aucun contrôle sur les listes de diffusion ou sur les listes des appels émis et reçus par les représentants du personnel et les représentants syndicaux dans le cadre de leur mandat, garantissant ainsi toute impossibilité d'utilisation détournée, notamment sur l'opinion d'un agent à l'égard d'une organisation syndicale voire son appartenance, ou sur le choix opéré, d'accepter ou non de recevoir des messages à caractère syndical.

16 RAPPEL DES PRINCIPAUX TEXTES APPLICABLES

Sans préjudice des évolutions futures et à titre d'information, à la date de la publication du présent document, les principaux textes applicables sont :

Code Civil, et notamment :

- article 9 relatif au droit au respect de la vie privée ;
- article 1366 relatif à la force probante de l'écrit électronique ;
- article 1367 relatif à la signature électronique.

Code Pénal, et notamment :

- article 226-15 sur l'atteinte au secret des correspondances ;
- articles 226-16 à 226-24 et R. 625-10 à R. 625-13 relatifs aux atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques ;
- articles 323-1 à 323-7 relatifs aux atteintes aux systèmes de traitement automatisé de données ;
- article 432-9 relatif aux atteintes portées au secret des correspondances par les personnes dépositaires de l'autorité publique ou chargées d'une mission de service public.

Code de la Propriété Intellectuelle (première partie relative à la propriété littéraire et artistique), et notamment :

- articles L. 131-3-1 à L. 131-3-3 relatifs au droit d'auteur des agents publics.

Code des Postes et des Communications Électroniques (livre II relatif aux communications électroniques)

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

Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD)

Loi n° 2004-575 du 21 juin 2004 (LCEN) pour la confiance dans l'économie numérique.

Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.

Loi n° 84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale.