Conseil Communautaire
27 juin 2019
Abergement-la-Ronce – 18h30

DÉLIBERATION

Nombre de conseillers en exercice : 84
Nombre de délégués titulaires ou suppléants présents : 58
Nombre de procurations : 14
Nombre de votants : 72
Date de la convocation : 20 juin 2019
Date de publication : 5 juillet 2019

Délégués présents (titulaires et éventuellement suppléants) : J.L Bouchard, D. Bernardin, J.M Mignot suppléé par T. Gauthray-Guyenet, B. Guerrin, B. Chevaux suppléé par C. Clairotte, J.C Robert, R. Pouthier, B. Negrello suppléé par C. Bardoux, G. Fumey, O. Meugin, P. Verne, R. Foret, J.C Lab, A. Albertini, C. Crétet, M. Giniès, F. Barthoulot, C. Bourgeois-République, S. Champanhet, J.P Cuinet, C. Demortier, T. Druet, J.P Fichère, J.B Gagnoux, I. Girod, J. Gruet, P. Jaboviste, N. Jeannet, A. Maire-Amiot, I. Mangin, S. Marchand, C. Nonnotte-Bouton, J. Péchinot, J.M Sermier, J.C Wambst, S. Calinon, J.L Croiserat, F. Macard, L. Bernier, J. Lombard, G. Jeannerod, A. Diebolt, J. Thurel, M. Henry, A. Courderot, D. Troncin, D. Baudard suppléé par C. Labourot, D. Pernin, E. Saget, F. David, G. Fernoux-Coutenet, J. Regard, C. François, G. Coutrot suppléé par G. Ginet, J.M Daubigney, P. Tournier, M. Hoffmann, J. Lagnien.

Délégués absents ayant donné procuration : P. Blanchet à J. Thurel, M. Berthaud à J. Gruet, I. Delaine à C. Bourgeois-République, F. Dray à P. Jaboviste, D. Germond à C. Nonnotte-Bouton, A. Hamdaoui à T. Druet, P. Jobez à J Péchinot, S. Kayi à N. Jeannet, J.P Lefèvre à J.P Cuinet, P. Roche à I. Mangin, E. Schlegel à J.M Sermier, P. Jacquot à M. Hoffmann, M. Boué à J.M Daubigney, J. Drouhain à C. Hanrard.

Délégués absents non suppléés et non représentés : G. Soldavini, D. Michaud, G. Chauchefoin, S. Hédin, J. Zasempa, J. Dayet, M. Jacquot, D. Chevalier, C. Mathez, E. Saget, V. Chevriaut, R. Curly.

GRAND DOLE
Communauté d'agglomération
Place de l'Europe
BP 458 – 39109 DOLE CEDEX
Tel 03.84.79.78.40
Fax 03.84.79.78.43
info@grand-dole.fr
www.grand-dole.fr

Référence
N°GD 65/19b

Objet
Adoption de la charte d'utilisation du système d'information de la Communauté d'Agglomération du Grand Dole et de la Ville de Dole

Secrétaire de séance
René POUTHIER

Rapporteur :
Stéphane CHAMPANHET

Vu le règlement européen 2016/679 du 27 avril 2016 sur la protection des données (RGPD),

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée et ses textes d'application,

Vu l'avis favorable du Comité Technique du 17 juin 2019,

Considérant les orientations stratégiques de la Communauté d'Agglomération du Grand Dole visant à maintenir l'intégrité de son système d'information,

La Communauté d'Agglomération du Grand Dole dispose d'un système d'information et de communication nécessaire à l'exercice de ses missions et compétences ; dans ce cadre, elle permet à son personnel d'utiliser des moyens de communication électronique, ainsi que des ressources informatiques, informationnelles, numériques et technologiques.

Ces différents outils offrent également à leurs utilisateurs une ouverture vers l'extérieur ; si leur utilisation est faite à bon escient, ainsi que dans le respect des usages et de la législation en vigueur, ces outils peuvent être des vecteurs de modernisation de la collectivité et du service public. Une mauvaise utilisation de ces outils peut, au contraire, engendrer des risques d'atteinte à la confidentialité, à la disponibilité et à l'intégrité de l'information, et engager ainsi la responsabilité civile et/ou pénale de l'utilisateur et de la collectivité.

Rendu exécutoire par télétransmission en Préfecture le 06 juillet 2019
N° identifiant : 039-200010650-20190627-6519b-DE

GRAND DOLE
Communauté d'agglomération

La présente charte d'utilisation du système d'information, validée par le Comité Technique en date du 17 juin 2019, s'inscrit dans une démarche d'information, de sensibilisation et de responsabilisation des utilisateurs sur les moyens de communication électronique et le système d'information de la Communauté d'Agglomération du Grand Dole.

Après en avoir délibéré, le Conseil Communautaire, à l'unanimité des membres présents et représentés :

- **ADOPTE** la charte d'utilisation du système d'information de la Communauté d'Agglomération du Grand Dole et de la Ville de Dole, telle que présentée en annexe.

Fait à Abergement-la-Ronce,
Le 27 juin 2019
Le Président, Jean-Pascal FICHERE,

Une copie de la présente délibération sera transmise à :
- Direction Pilotage et Coordination
- Pôle MR / Direction des Finances
- Pôle MR / Direction des Systèmes d'Information
- Trésorerie Municipale du Grand Dole

Rendu exécutoire par télétransmission en Préfecture le 06 juillet 2019
N° identifiant : 039-200010650-20190627-6519b-DE

CHARTE D'UTILISATION DU SYSTÈME D'INFORMATION DE LA COMMUNAUTÉ D'AGGLOMÉRATION DU GRAND DOLE ET DE LA VILLE DE DOLE

1. Introduction

Depuis le 1er janvier 2012, les services de la Ville de Dole et de la Communauté d'Agglomération du Grand Dole sont mutualisés. Depuis cette date, les collectivités disposent d'un système d'information unique qui regroupe toutes les ressources informatiques qu'elles soient effectivement partagées ou spécifiques à l'une ou l'autre collectivité.

2. Objet de la charte

La présente charte a pour objet de définir les règles de bonne utilisation des ressources informatiques de la Ville de Dole, du Centre Communal d'Action Sociale de Dole et de la Communauté d'Agglomération du Grand Dole.

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

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

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

3. Champ d'application de la charte

La charte s'applique à tout utilisateur du système d'information des collectivités.

Est considérée comme « utilisateur », toute personne, quel que soit son statut (élu, agent des collectivités, stagiaire, enseignant, consultant extérieur, prestataire, etc ...) autorisée à utiliser, consulter et modifier le système, de façon temporaire ou permanente.

En qualité d'utilisateur du système d'information, chacun s'engage à appliquer l'ensemble des dispositions de la présente charte.

La mise en place de la présente charte a été validée par les assemblées délibérantes des différentes collectivités : Ville de Dole : délibération ....
CCAS de la Ville de Dole : délibération ....
Communauté d'Agglomération du Grand Dole : délibération ....
Préalablement, le Comité Technique commun a été saisi le XXX

Rendu exécutoire par télétransmission en Préfecture le 06 juillet 2019
N° identifiant : 039-200010650-20190627-6519b-DE

4. Règles d'utilisation du système d'information

L'utilisateur est responsable de l'usage qu'il fait des ressources du système d'information dans l'exercice de ses fonctions.
Il doit réserver l'usage de ces ressources au cadre de son activité professionnelle.
Toutefois, un usage privé raisonnable, notamment de la messagerie professionnelle, limité aux nécessités de la vie courante et familiale est toléré. Cet usage ne doit ni affecter le fonctionnement des systèmes ni perturber l'activité professionnelle. Une consultation ponctuelle et limitée, pour motif personnel, des sites Internet dont le contenu n'est pas contraire à l'ordre public, aux bonnes mœurs et ne mettant pas en cause l'intérêt et la réputation de l'institution, est ainsi tolérée.

Pour accéder au système d'information, l'utilisateur doit utiliser prioritairement les moyens fournis par les collectivités. L'usage d'autres outils, notamment du matériel personnel, pour accéder au système d'information doit être soumis préalablement à l'autorisation de la DSI. L'utilisation à destination professionnelle d'outils personnels est à l'initiative de l'utilisateur et reste de sa responsabilité ; les collectivités ne pourront être tenues responsables en cas de dégradation de ces matériels.

Tenu au devoir de réserve, à l'obligation de discrétion professionnelle et au secret professionnel, l'utilisateur ne doit pas divulguer sans autorisation les informations auxquelles il a accès, ou si elles sont de nature à porter préjudice aux collectivités ou à une personne physique.
L'obligation de réserve implique, de plus, que les agents fassent preuve de retenue dans les opinions exprimées dans et en dehors de leur temps de travail, et notamment dans les réseaux sociaux, afin de ne pas nuire à l'image du service public.

L'utilisateur ne doit pas non plus tenter d'accéder aux informations pour lesquelles il n'est pas habilité.

4.1. Respect du cadre législatif et réglementaire

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

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

Il est interdit d'accéder, de télécharger, de stocker, de distribuer des informations portant atteinte à la dignité humaine (pornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée).
L'inscription sur de tels sites avec l'adresse mail professionnelle de l'utilisateur est proscrite.
Si l'utilisateur est amené à recevoir, à son insu, de tels éléments, il est tenu de les détruire aussitôt.
L'utilisateur doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents sous forme d'informations, d'images, de vidéos, de fichiers ou autres.

Il est interdit d'utiliser les ressources du système d'information à des fins de harcèlement, menace ou d'injure, et de manière générale à violer les lois en vigueur.

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

Il est interdit de falsifier un fichier source pour un usage détourné.

4.2. Protection des données à caractère personnel

Le règlement européen 2016/679 du 27 avril 2016 sur la protection des données (RGPD) applicable à compter du 25 avril 2018 définit les conditions dans lesquelles le traitement des données à caractère personnel peut être effectué.
Ce règlement remplace la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Il permet de garantir les droits des personnes concernées par l'ensemble des traitements de leurs données personnelles : droits d'accès, droits de rectification, droits d'opposition, droits à la limitation du traitement, droit à l'oubli, droit à l'effacement des données, droit à la portabilité des données.

Les collectivités ont désigné un délégué à la protection des données à caractère personnel également nommé DPO. Ce dernier a pour mission de veiller au respect des dispositions du Règlement Général sur la Protection des Données (RGPD).

Dans le cadre de son activité, l'utilisateur peut avoir besoin de traiter des données à caractère personnel. Aussi, préalablement à la constitution de ce fichier, il devra se rapprocher de sa direction (le responsable du traitement) et du DPO pour s'assurer de la conformité du traitement de ces données au RGPD.

Le responsable du traitement, aidé du DPO, recense dans un registre la liste des traitements de données à caractère personnel des différentes collectivités au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande.

Le DPO veille au respect des droits des personnes concernées par les traitements et est habilité à recevoir les demandes et réclamation concernant l'ensemble des données à caractère personnel. En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le DPO (Jean-Luc DOLE, dpo@grand-dole.fr).

Il est formellement interdit de procéder à la collecte de données nominatives en dehors des traitements déclarés dans le cadre du RGPD.
Il est rappelé que toute divulgation, en dehors du service responsable du traitement, d'informations nominatives touchant à la vie privée, peut être susceptible de poursuites pénales.
Il est interdit de collecter des données par un moyen frauduleux, déloyal ou illicite.

4.3. Les modalités d'intervention de la DSI

La DSI assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication des collectivités. Les agents de ce service disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.
Ils sont assujettis au devoir de réserve, à l'obligation de discrétion professionnelle et au secret professionnel et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

- Création de compte

A l'arrivée d'un nouvel utilisateur dans la collectivité, la DSI lui fournira les identifiants de son compte, qui lui permettra d'avoir accès aux ressources informatiques. Ce compte est composé d'un nom d'utilisateur et d'un mot passe.
Le mot de passe fourni par la DSI est temporaire, l'utilisateur devra le changer lors de sa première connexion.
Pour être efficace, le mot de passe doit comporter au minimum 8 caractères alphanumériques et doit mixer un maximum de type de caractères différents (au minimum 3) : minuscules, majuscules, chiffres, caractères spéciaux (+, -, *, /, !, #, $, :, %...).
Le mot de passe doit obligatoirement être modifié tous les 6 mois.
Une fois le mot de passe modifié, l'utilisateur est le seul à le connaitre (la DSI n'en a plus connaissance). Ce mot de passe doit rester confidentiel.

- Prise en main et observation à distance

La DSI dispose d'un outil de prise en main à distance pour dépanner les utilisateurs. Ces prises en main et observations à distance se feront toujours avec l'accord de l'intéressé. Il est averti par un message en anglais à l'écran qu'une tentative de prise en main est en cours. L'utilisateur doit approuver cette demande pour que la prise en main puisse démarrer.

- Suppression des droits utilisateurs

Au départ d'un utilisateur, la DSI procède à la désactivation du compte de l'utilisateur (suppression de ses accès informatiques sur le système d'information des collectivités).

4.4. Les mesures de sécurité à prendre

- Authentification

Pour se connecter au système d'information, l'utilisateur doit entrer ses informations de connexion (identifiant et mot de passe). Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

- Règles de sécurité

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

- Modifier son mot de passe tous les 6 mois (une historisation des deux derniers mots de passe est faite afin d'obliger les utilisateurs à ne pas remettre les mêmes) ;
- Ne jamais confier son identifiant/mot de passe à un tiers y compris ses collègues ou son supérieur hiérarchique ;
- Ne jamais demander l'identifiant/mot de passe à un collègue ou subordonné ;
- Ne pas laisser en évidence les informations de compte utilisateur (identifiant et mot de passe) si ces informations sont conservées sous forme écrite ;
- Verrouiller son ordinateur à chaque départ de son poste de travail ;
- Protéger l'accès aux ressources informatiques (matérielles, logicielles, ...) par un mot de passe dès lors que c'est possible, y compris pour les téléphones portables ;

- Ne pas utiliser les identifiants et mot de passe d'une autre personne, ce qui est considéré comme de l'usurpation d'identité ;
- Ne pas laisser à disposition des supports informatiques amovibles (disque dur externe, CD-Rom, clé USB) contenant des données confidentielles ;

- Sauf exception validée par la DSI, l'utilisation des supports amovibles de type clé USB doit être limitée au transfert de données entre matériels qui ne sont pas connectés au même réseau. Le support amovible doit être vidé de tout contenu après utilisation pour éviter la propagation de données sensibles en cas de perte ou de vol.

4.5. Matériels, progiciels, logiciels, données

L'utilisateur s'interdit de modifier les équipements mis à sa disposition par les collectivités, notamment par l'ajout de logiciels sur les postes de travail. Toute tentative de désinstallation est proscrite, celle-ci pouvant provoquer un dysfonctionnement du poste de travail. A des fins de précaution, certaines configurations de postes de travail peuvent être verrouillées par la DSI.

Le poste de travail de chaque utilisateur est protégé par un logiciel antivirus.
Cependant, l'utilisation des applications communicantes (Internet, messagerie) et des supports de stockage (disque dur externe, CD-Rom, clé USB) peut, malgré les précautions prises, provoquer la transmission et l'installation sur le poste de travail de l'utilisateur, à l'insu de ce dernier, de programmes ou fichiers, qui altèrent ou pillent les données et logiciels qu'il contient.
En cas d'anomalie, l'utilisateur doit stopper toute transaction, quitter les applications en cours, arrêter son poste de travail, et prévenir immédiatement la DSI.

Le stockage de documents privés sur les espaces partagés (serveurs, Drive et intranet) est interdit.

L'utilisateur est informé que :

- Tout document stocké sur une ressource mise à disposition par les collectivités est réputé professionnel SAUF s'il est stocké dans un répertoire portant la mention « Personnel et Confidentiel » ;
- Le fonctionnement du poste de travail ne doit pas être altéré par le stockage de documents privés ;
- Les documents privés stockés doivent respecter le cadre légal et réglementaire ;
- Les disques des postes de travail ne sont pas sauvegardés. Par conséquent, les documents privés stockés sur ces disques peuvent être définitivement perdus sans que la responsabilité des collectivités puisse être engagée ;
- Pour les postes de travail pouvant être partagés entre plusieurs utilisateurs, seuls les documents enregistrés dans le répertoire « Mes documents » ne seront accessibles que par l'utilisateur.

Afin de préserver le bon fonctionnement et la cohérence du Système d'Information, tout choix de logiciel ou progiciel amené à être installé dans le parc informatique ne pourra se faire qu'avec l'accord préalable de la DSI.

Les utilisateurs connectés au réseau disposent de plusieurs moyens d'impression, suivant leur localisation géographique. L'implantation de ces matériels est définie par la DSI, en relation avec les directions concernées.

Toute installation ou déménagement de poste de travail doit se faire avec l'accord préalable des services techniques compétents et de la DSI, notamment en ce qui concerne les branchements électriques et informatiques.

4.6. Respect du matériel

Il convient de préserver le matériel appartenant aux collectivités, soit :

- Éteindre son poste par arrêt logiciel pour terminer proprement ses sessions (hors cas de blocage technique) ;
- Éteindre son poste par arrêt logiciel la nuit et le week-end, et plus généralement durant toute absence prolongée (sauf demande expresse de la DSI) ;
- En cas de perte ou de vol, avertir immédiatement votre responsable de service et la DSI ;
- Éviter la consommation de nourriture, boissons, et de manière générale toute utilisation de substance pouvant endommager le matériel ;
- Prendre soin des appareils mobiles (téléphone, smartphone, ordinateur portable, ...) qui sont particulièrement fragiles et convoités.

En cas de dégradation ou de vol de matériel et si un non-respect des consignes de sécurité est avéré, les collectivités se réservent le droit de demander le remboursement de tout ou partie des frais occasionnés pour la réparation ou le remplacement du matériel endommagé.

4.7. Utilisation de la messagerie

Depuis 2016, les utilisateurs ayant besoin d'une messagerie électronique se voient attribuer un compte Google « G suite ». Ce compte donne accès principalement à une adresse de messagerie (Gmail), à un service d'agenda (Google Agenda) et à un espace de stockage permettant également de partager certaines données (Drive). Cette solution de « cloud » stocke les données sur le réseau de centre de données sécurisé de Google.
Ce compte Gmail est uniquement accessible par Webmail.
En aucun cas la DSI n'a accès à la messagerie, et plus généralement au compte « G suite » des utilisateurs.

- Règles générales d'utilisation

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

La messagerie dispose d'un outil anti-virus et de filtrage qui élimine automatiquement tout message suspect. Néanmoins l'utilisateur doit rester vigilant et ne devra pas ouvrir les courriels qui lui paraissent suspects.

L'utilisation de la messagerie est réservée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée de manière ponctuelle pour répondre aux besoins de la vie quotidienne.
Tout message est considéré comme professionnel sauf s'il porte la mention « personnel ». Dès lors les collectivités s'interdisent de consulter ces messages.

L'utilisateur doit être conscient qu'un message électronique peut être stocké, réutilisé, exploité à des fins auxquelles l'utilisateur n'aurait pas pensé en le rédigeant. Il peut constituer une preuve ou un

Rendu exécutoire par télétransmission en Préfecture le 06 juillet 2019
N° identifiant : 039-200010650-20190627-6519b-DE

commencement de preuve par écrit. Par conséquent, une grande prudence est à observer dans l'utilisation du courrier électronique à destination des tiers.

L'utilisateur doit utiliser avec discernement les listes de diffusion personnelles ou collectives. Il doit éviter l'envoi de copies à un nombre injustifié de destinataires. Il ne doit pas diffuser de l'information non souhaitée par les destinataires (SPAM).

- En cas d'absence de l'utilisateur :

En cas d'absence prévisible, l'utilisateur doit activer l'option de répondeur automatique indiquant sa période d'absence, en précisant le service ou la personne qui doit pouvoir gérer ses dossiers pendant son absence.
En cas d'absence inattendue d'un utilisateur (arrêt maladie...), le responsable de service, pour assurer le bon fonctionnement de son service, doit contacter son agent pour qu'il active l'option de répondeur automatique. Si l'agent est dans l'incapacité d'activer le répondeur automatique, son chef de service peut demander à la DSI, après accord écrit de son supérieur, d'activer le répondeur automatique de l'agent pour signaler son absence et indiquer le nom et l'adresse mail du collègue qui va le remplacer pendant son absence. A cette fin, la DSI doit réinitialiser le mot de passe du compte de l'utilisateur absent pour pouvoir accéder à sa messagerie.

- Départ définitif :

Lors de son départ, l'utilisateur devra se rapprocher de la DSI pour mettre en place le suivi de sa messagerie et le transfert des messages importants sur la messagerie d'un de ses collègues. Si l'utilisateur ne s'est pas rapproché de la DSI avant son départ, son responsable peut demander à la DSI l'accès à sa messagerie pour récupérer les messages nécessaires au bon fonctionnement de son service. Son compte Google « G suite » sera définitivement supprimé un mois après son départ.

- Accès au Drive :

Lors de la création du compte Google « G suite » de l'utilisateur, la DSI pourra donner l'accès à l'option Drive, si l'utilisateur en a besoin. Avec Google Drive, les utilisateurs peuvent stocker des fichiers dans le « cloud » de Google, les partager avec d'autres utilisateurs et y accéder depuis un ordinateur en dehors des collectivités. L'utilisateur reste seul responsable des fichiers qu'il décide de partager et de la façon dont il les partage. En cas de doute sur la façon de partager un document, la DSI doit être contactée.
Lors de son départ, l'utilisateur devra se rapprocher de la DSI pour mettre en place le transfert de son Drive.

4.8. Recommandations spécifiques aux utilisateurs en situation de mobilité

Afin de préserver la confidentialité des données stockées sur les disques locaux et d'assurer la sécurité des matériels appartenant aux collectivités, il est demandé, dans le cadre de déplacements professionnels, de respecter les consignes suivantes :

- Éviter toute imprudence ou toute mauvaise utilisation qui pourrait engager votre responsabilité personnelle ;
- Ne pas exposer le matériel à des conditions climatiques agressives (humidité, soleil etc...) ;
- Ne pas laisser le matériel sans surveillance (dans les transports en commun par exemple) ;
- Ne pas prêter le matériel ;
- Tout ordinateur portable mis à disposition doit être rendu exclusivement à la DSI à la fin de son utilisation. Il est rappelé à l'utilisateur qu'il a la responsabilité du matériel qui lui est confié

Rendu exécutoire par télétransmission en Préfecture le 06 juillet 2019
N° identifiant : 039-200010650-20190627-6519b-DE

jusqu'au retour à la DSI. En particulier pour les réunions en fin de journée, le matériel ne doit, ni être laissé en salle de réunion, ni déposé à l'accueil de l'hôtel de ville ;
- Supprimer tous les fichiers temporaires de l'ordinateur portable ;
- Dès que le matériel est connecté au système d'information de la collectivité : enregistrer les documents modifiés sur les espaces de stockage sécurisés ;
- Supprimer tous les documents non indispensables pour éviter les risques de divulgation d'informations stratégiques en cas de perte ou de vol du matériel.

4.9. Organisation des espaces de stockage des documents bureautiques

La DSI met à disposition des utilisateurs connectés au réseau principal des collectivités plusieurs espaces de stockage du réseau organisés selon la destination des fichiers :

- Direction/Service : cet espace est accessible aux agents de la structure ; c'est l'espace dans lequel doivent être stockés les documents professionnels susceptibles d'être partagés au sein du service ;
- Transfert : cet espace est accessible à tous les agents ; c'est un espace qui permet de partager des documents entre services. Ce n'est pas un espace de partage ou de travail permanent. Cet espace ne doit pas comporter de documents confidentiels qui ne soient pas protégés par des mots de passe.

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

- Organiser le volume bureautique de façon générique (éviter les répertoires individuels, nommés avec le nom ou le prénom d'une personne) de manière à faciliter les recherches. Chaque service doit créer sa propre arborescence en fonction de ses missions ;
- Supprimer les fichiers obsolètes ou sans intérêt de manière à récupérer de l'espace disque sur le serveur bureautique ;
- Dans la mesure du possible, aucun document ne doit être stocké localement sur le disque dur du poste de travail : ces données ne sont pas sauvegardées. En cas de vol aucune confidentialité ne peut être garantie ;
- Le disque dur du poste de travail de l'utilisateur et les espaces de stockage du réseau ne doivent pas contenir de programmes, logiciels, documents, fichiers, informations ou données, ne respectant pas la législation en vigueur ;
- L'accès aux données personnelles et confidentielles ne pourra être réalisé qu'en cas de risque ou évènement particulier, et en présence de l'utilisateur, à sa demande ou après l'avoir convoqué à cette fin ;
- Lors de son départ, l'utilisateur devra supprimer les données d'ordre personnel. Les données d'ordre professionnel devront être transmises aux agents du service reprenant les dossiers ou mises à disposition du remplaçant ;
- Toutes les informations relatives à l'utilisateur seront supprimées après son départ par les administrateurs systèmes et réseaux de la DSI.

La DSI assure la sauvegarde des données enregistrées dans les espaces de stockage « S:\Services ». Les documents situés en dehors de ces espaces de stockage réseau (le poste de travail) ne sont pas sauvegardés.

Afin de garantir la pérennité, la sécurité et l'accessibilité des données, il est formellement proscrit de stocker ces données en dehors du système d'information des collectivités ("cloud" internet, Dropbox, stockages externalisés, ...).

Rendu exécutoire par télétransmission en Préfecture le 06 juillet 2019
N° identifiant : 039-200010650-20190627-6519b-DE

Pour donner un accès ponctuel à un tiers extérieur, il est préférable d'utiliser le service Google Drive accessible via les comptes « G suite ».

L'utilisation d'espaces de travail collaboratifs mis à disposition par des partenaires est soumise à autorisation de la DSI. Dans ce cas, l'utilisateur reste seul responsable des informations mises à disposition sur l'espace de travail.

4.10. Utilisation d'Internet

Chaque agent est responsable de l'usage qu'il fait d'Internet, et plus particulièrement du choix des sites visités.
L'utilisateur doit veiller à ne pas perturber le fonctionnement général du système d'information par un usage abusif des accès à Internet.

Il est rappelé que la plupart des sites Internet visités gardent une trace de chaque passage. L'attention de l'utilisateur est attirée sur ce point et il lui est demandé de prendre toutes les précautions à cet égard.

L'utilisateur engage sa responsabilité personnelle en ce qui concerne les sites visités et le contenu de ceux-ci.
L'attention des utilisateurs est appelée sur le fait que tout téléchargement peut comporter certains risques juridiques (voir chapitre correspondant) et techniques notamment l'introduction de virus malgré les dispositions prises à travers les dispositifs de sécurité mis en œuvre par la DSI.
Pour des raisons techniques, l'historique des connexions Internet des utilisateurs est enregistré. Ces informations sont conservées pendant 6 mois et sont susceptibles d'être communiquées, sur décision judiciaire, aux services de police.
A des fins de statistiques, de qualité de service et de sécurité, le trafic Internet pourra faire l'objet d'une supervision ou de vérifications par les collectivités, dans les limites prévues par la loi.

4.11. Utilisation des logiciels ou progiciels métiers

Les collectivités mettent à la disposition de l'utilisateur des ressources (Intranet, Extranets, logiciels, progiciels ...) pour exercer son activité professionnelle, conformément aux règles juridiques et techniques applicables et aux prescriptions définies.
Les habilitations applicatives sont déterminées par la direction gestionnaire de l'outil concerné. Elles sont liées aux fonctions occupées et peuvent de ce fait évoluer dans le temps.
Les informations de connexion sont strictement personnelles et ne peuvent en aucun cas être transférées, même temporairement, à un tiers.

4.12. Utilisation de la téléphonie fixe

Le téléphone fixe est un outil mis à la disposition de l'utilisateur à titre professionnel. Une tolérance pour des usages personnels et occasionnels est acceptée, de manière très limitée.
L'agent peut disposer d'un poste téléphonique avec un numéro nominatif identifié.
L'utilisateur bénéficie du droit absolu au secret des communications téléphoniques qui s'applique à l'ensemble des messages émis et reçus par le biais de son poste téléphonique.

4.13. Utilisation de la téléphonie mobile

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

4.13.1. Téléphone de service

Le téléphone est partagé par plusieurs utilisateurs (astreintes, déplacements, ...). Une tolérance pour des usages personnels et occasionnels est acceptée, de manière très limitée. L'utilisateur est responsable du matériel et doit notamment :

- Informer la DSI de toute anomalie sur le matériel ;
- Rendre le matériel en bon état de fonctionnement pour l'utilisateur suivant (appareil propre, batterie chargée, accessoires présents, ...) ;
- Ne pas stocker d'informations personnelles (photos, contacts, ...) sur les téléphones de service ;
- Ne pas installer d'application sur les téléphones de service sans accord préalable de la DSI ;
- Ne pas transférer les appels vers un téléphone portable n'appartenant pas aux collectivités (le transfert d'appel vers un téléphone fixe est autorisé).

4.13.2. Téléphone attribué

L'utilisateur est responsable du matériel qui lui est attribué et de l'utilisation qui en est faite (notamment la consultation de sites internet sur les smartphones).
L'utilisateur doit notamment :

- Informer la DSI de toute anomalie sur le matériel ;
- Informer la DSI de toute modification d'utilisation professionnelle pouvant entraîner des surcoûts (déplacements professionnels à l'étranger, envoi de SMS en masse, ...). Dans l'idéal, l'information doit être donnée à la DSI un mois avant que la modification de situation soit effective ;
- Pour les terminaux de type Smartphone, protéger le verrouillage de l'écran par un code ou un mot de passe ;
- Supprimer les informations personnelles (mails, SMS, photos, contacts, ...) avant de restituer son téléphone.

Les collectivités n'ont pas accès au détail des communications de l'utilisateur en vertu du droit à la protection de la vie privée.

4.13.3. Téléphone personnel

Les collectivités donnent la possibilité aux utilisateurs possédant une adresse email professionnelle nominative de la configurer sur leur téléphone personnel. Pour permettre cette connexion, la politique de sécurité impose aux utilisateurs de protéger leur téléphone personnel par un mot de passe.
La configuration d'une adresse email non nominative n'est pas autorisée.

Pour mettre en œuvre cette connexion, l'utilisateur devra contacter la DSI.

4.14 Utilisation de photographies

Les agents ne peuvent diffuser, hors du cadre strictement professionnel, les photographies prises dans l'accomplissement de leur mission.

5. Droits des utilisateurs

Afin d'assurer la sécurité du système d'information ainsi que le respect des règles définies ci-dessus et de disposer de données statistiques, les collectivités ont mis en place les outils de surveillance et de contrôle suivants :

- Identification et filtrage des références des émetteurs et des destinataires des messages ou fichiers ;
- Contrôle et filtrage anti-virus ;
- Contrôle et filtrage du type de fichiers joints émis et réceptionnés ;
- Contrôle de la taille des fichiers émis, réceptionnés et stockés et filtrage des fichiers ;
- Filtrage des sites accessibles ;
- Liste des sites Internet ayant été visités par l'utilisateur avec horodatage de la connexion.

Les contrôles pourront être effectués de manière permanente ou ponctuelle en fonction des besoins, des risques ou des incidents détectés. Les données collectées seront traitées par le directeur des Systèmes d'Information ou le Directeur Général des Services en fonction de la nature des incidents détectés. Elles seront conservées pour une durée de 1 an, conformément aux exigences de la Commission Nationale de l'Informatique et des Libertés (CNIL).
Ces moyens de contrôle seront mis en œuvre dans le respect de la réglementation en vigueur.
Conformément aux articles 39 et 40 de la Loi Informatique et Liberté du 6 janvier 1978, l'utilisateur dispose d'un droit d'accès et de modification des informations le concernant et issues de ces contrôles. L'exercice de ce droit est applicable auprès de la Direction des Ressources Humaines.

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

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

Rendu exécutoire par télétransmission en Préfecture le 06 juillet 2019
N° identifiant : 039-200010650-20190627-6519b-DE

6. Références légales et législatives

- Règlement européen 2016/679 du 27 avril 2016 sur la protection des données (RGPD) ;
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée et ses textes d'application ;
- Code Pénal : dispositions relatives aux atteintes aux droits de la personnalité résultant des fichiers ou des traitements informatiques (articles 226-15 à 24), dispositions relatives aux atteintes aux systèmes de traitement automatisés de données (articles 323-1 à 323-7) et dispositions relatives à la responsabilité pénale de la personne morale (article 323-6) ;
- Loi du 3 juillet 1985 sur la protection des logiciels par le droit d'auteur et loi du 1er juillet 1992 relative au Code de la Propriété Intellectuelle (CPI) ;
- Loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications ;
- Code du Travail, notamment article L1121-1 (principe de proportionnalité), article L 1121-9 (information-consultation préalable du Comité d'Entreprise sur la mise en œuvre de moyens de contrôle des salariés), article L 1222-4 (obligation d'informer le salarié ou candidat à l'emploi sur dispositif informatisé le concernant, article L 2323-32 (information-consultation du Comité d'entreprise pour l'introduction de nouvelle technologie modifiant les conditions de travail) ;
- Loi n°96-659 du 26 juillet 1996 : réglementation des télécommunications et décrets d'application sur la cryptologie ;
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
- Loi n°84-53 du 26 janvier 1984 (art. 89 et 90) et le décret n° 89-677 du 18 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux ;
- Décret n°92-1194 du 4 novembre 1992 (art. 6) fixant les dispositions communes applicables aux fonctionnaires stagiaires de la Fonction Publique Territoriale ;
- Décret n°88-145 du 15 février 1988 (art. 36 et 37) relatif aux agents contractuels ;
- Décret n°91-298 du 20 mars 1991 (art. 15) relatif aux agents à temps non complet.

Rendu exécutoire par télétransmission en Préfecture le 06 juillet 2019
N° identifiant : 039-200010650-20190627-6519b-DE