Mairie de GRUSON

Charte des usages numériques et de la protection des données de la commune

Table des matières

1 INTRODUCTION

De nouvelles pratiques de travail et formes de communication sont présentes dans l'environnement professionnel. Il est observé un développement croissant des réseaux, une multiplicité des supports (tablette, smartphone, pc portable...), des usages des technologies de l'information et une émergence du télétravail. Cela induit une organisation et une gestion différentes dans les relations au sein de la commune, entre les agents mais également entre les agents et les usagers.

La commune est exposée à des responsabilités importantes dans le cadre de ses nombreuses activités, des actions menées par les services et les agents et notamment vis-à-vis des moyens qui leurs sont affectés au quotidien dans le cadre de leur activité professionnelle. **Devant l'essor des outils numériques permettant la collecte et le stockage de données à caractère personnel et le développement croissant des menaces de piratage informatique, il convient d'acquérir les bons réflexes et un cadre dans nos pratiques numériques.**

La présente charte n'a pas vocation à être un recueil des textes de loi, de référentiels de l'administration ou de normes spécifiques qu'il conviendrait de respecter. Il s'agit d'un **guide spécifique pour la commune présentant des règles de déontologie et de sécurité qui s'imposent à tous les utilisateurs quel que soit leur statut** (élus, utilisateurs titulaires ou utilisateurs non titulaires), y compris les intérimaires, les stagiaires et les saisonniers. Chaque utilisateur veille à faire accepter valablement les règles posées dans la charte à toute personne à laquelle il permettrait d'accéder aux ressources informatiques et de communication. **Son application au quotidien est l'affaire de tous, dans l'intérêt de chacun.**

Elle a pour objectifs :

- De définir l'ensemble des bonnes pratiques d'utilisation des ressources informatiques et de communication ;
- De faire appel au bon sens et à la responsabilité individuelle ;
- De préserver l'intérêt général et individuel ;
- De préserver un environnement de travail professionnel ;
- De garantir l'intégrité du système informatique et de l'ensemble des outils mis à disposition ;
- De protéger les informations que la commune détient,
- De limiter les risques de recherche de responsabilités pénales et civiles de chacun.

2 RÈGLES D'UTILISATION

2.1 Du matériel informatique et des logiciels

L'utilisateur est responsable du matériel informatique (ordinateur, imprimante, tablette, smartphone, …) et des logiciels qu'il manipule dans le cadre de l'exercice de ses fonctions. Il doit donc veiller à leur protection en faisant preuve de prudence et notamment, il doit :

- Enregistrer régulièrement ses documents de travail pendant leur utilisation ;
- Verrouiller/bloquer l'accès en cas d'absence, même temporaire. Le verrouillage automatique du matériel informatique après quelques secondes ou minutes d'inactivité doit être activé. L'utilisateur pourra ensuite accéder au matériel informatique après avoir déverrouillé celui-ci (cf. 3.3 Mot de passe) ;

- Fermer les programmes informatiques et éteindre totalement le matériel informatique (ordinateur, écran, imprimante, …) lors d'absences prolongées (pause repas, départ quotidien, weekend, congés). L'utilisation de la mise en veille du matériel informatique est possible pour des absences courtes. L'utilisateur pourra ensuite accéder au matériel informatique après avoir déverrouillé celui-ci (cf. 3.3 Mot de passe) ;
- Utiliser les logiciels strictement nécessaires à l'exécution de ses missions ;
- Ne pas utiliser de messagerie (Email ou tchat) non mise à disposition par la commune pour l'exécution de ses missions. En effet, les messageries n'ayant pas contractualisé avec la commune ne disposent pas de garanties suffisantes en sécurité ;
- Ne pas rediriger sa messagerie professionnelle ou transférer des Emails professionnels vers une messagerie externe à la commune ;
- Éviter de connecter de nouveaux équipements sur le réseau (ordinateur personnel, ...) ou sur les ordinateurs de la commune (clé usb, ...) sans l'autorisation préalable de la ou des personnes en charge de l'informatique ;
- Eviter l'usage du wifi publics (hôtels, gares, restaurants, …) ;
- Ne pas copier sur le matériel informatique des fichiers susceptibles de créer des risques pour la sécurité de la commune (document vérolé, ...) ;
- Ne pas télécharger sur internet, reproduire ou diffuser sans autorisation de l'auteur, ou du propriétaire des droits d'exploitation, les œuvres littéraires, musicales, photographiques, audiovisuelles protégées par des droits de reproduction et de représentation. Bien qu'accessible facilement sur internet, les contenus multimédias ne sont pas forcément libres de droit.

2.1.1 Appartenant à la commune

Le matériel informatique et les logiciels confiés à l'utilisateur par la commune répondent à une exigence de bon fonctionnement pour permettre l'exécution des missions de l'utilisateur. Pour maintenir le bon fonctionnement du matériel informatique et des logiciels, l'utilisateur veillera à :

- Ne pas modifier le paramétrage et les caractéristiques du matériel informatique confié et notamment les dispositifs spécifiques aux mesures de sécurité (cf. *4.2 Mesures de sécurité mises en œuvre*) ;
- Ne pas installer de logiciels sur le matériel informatique. Cette mesure est normalement restreinte techniquement par la ou les personnes en charge de l'informatique. Dans l'éventualité où l'utilisateur doit installer un logiciel pour l'exercice de ses missions et en l'absence de support informatique, il doit en informer au préalable sa hiérarchie. Il est formellement interdit d'installer des logiciels dont la licence d'utilisation n'est pas autorisée dans la commune (logiciel piraté, logiciel gratuit, ...) ;
- Ne pas utiliser le matériel informatique et les logiciels de la commune à des fins commerciales ;
- Restituer son matériel informatique avant tout départ définitif. Les données à caractère privé auront été au préalable supprimées.

2.1.2 N'appartenant pas à la commune

La commune doit demeurer extrêmement vigilante sur les risques de perte de souveraineté et de contrôle sur les données qu'elle produit, collecte ou stocke.

L'utilisation de stockages ou d'applications (agenda, messagerie, …) sur internet non mis en œuvre par la commune n'est donc pas autorisée. En cas de nécessité, l'utilisateur se rapprochera de la ou les personnes en charge de l'informatique pour connaître la solution adaptée à ses besoins.

Non adaptée à une bonne protection des données, l'utilisation de matériel informatique personnel (ordinateur, tablette, téléphone, clé usb) est tolérée lorsque la situation ne permet pas de fonctionner autrement et uniquement après autorisation expresse et préalable de la personne responsable en charge de l'informatique.

Cependant, tout matériel informatique personnel utilisé dans un cadre professionnel devient une partie du système d'information de la commune. De ce fait, l'utilisateur doit veiller à la sécurité du matériel informatique employé et respecter autant que possible les règles de sécurité appliquées à l'utilisation du matériel informatique de la commune (cf. *2 Matériel informatique et logiciels de la commune*). Il veillera notamment à la sauvegarde des données professionnelles manipulées sur ce matériel informatique.

Les données professionnelles manipulées sur du matériel informatique n'appartenant pas à la commune restent la propriété de la commune.

2.1.3 Nomades (clé usb, téléphone portable, tablette, …)

Du matériel nomade peut être utilisé pour des besoins professionnels. De par sa nature, le matériel nomade présente un risque plus important de vol ou de perte, occasionnant également la perte des données qui y sont stockées. L'utilisateur sera donc vigilant lors de leur utilisation et devra :

- Limiter leur usage au strict nécessaire ;
- Ne conserver sur le matériel nomade que les données nécessaires aux besoins poursuivis ;
- N'utiliser du matériel nomade que pour un usage strictement professionnel ;
- Eviter d'y stocker des données sensibles (financière, médicale, …).

Lorsque l'utilisateur est amené à utiliser un support de stockage (clé usb, disque dur externe, …) pour des besoins professionnels (transfert de fichiers, …), il devra également :

- Limiter le déplacement des supports de stockage dans les locaux de la commune ou chiffrer au préalable les données avant de transmettre le support de stockage à l'extérieur de la commune ;
- Conserver les supports de stockage non utilisés dans un endroit fermé à clé ;
- Ne pas s'en servir comme support de sauvegarde.

Parce qu'un téléphone portable, un ordinateur portable ou une tablette sont souvent amenés à être utilisés en dehors des locaux de la commune, l'utilisateur devra porter une attention particulière à leur sécurité et au strict respect des règles de sécurité (cf *2.1 Du matériel informatique et des logiciels* et *2.1.4 A des fins privées*).

2.1.4 A des fins privées

Par « usage professionnel », on entend toute utilisation ayant un lien direct avec les activités pour lesquelles l'utilisateur a été recruté. Par opposition, on entend par « utilisation à titre privé », ou « usage non professionnel », les activités n'ayant aucun lien direct avec celles pour lesquelles l'utilisateur a été recruté.

Le matériel informatique et les logiciels de la commune sont mis à la disposition des utilisateurs à des fins professionnelles. Un usage à titre privé constitue une tolérance de la part de la commune. L'usage à titre privé (navigation sur internet, téléphone, …) doit être raisonnable (modéré), conforme aux règles et aux lois, non lucratif et à caractère exceptionnel. En outre, il doit s'inscrire dans le cadre des nécessités de la vie courante et familiale, sans affecter le bon fonctionnement de la commune, nuire à la performance de la ville ou encore à l'accomplissement des missions de service public.

Il convient de respecter à minima les règles d'utilisation suivantes lors d'une utilisation à titre privé :

- L'envoi d'un mail via la messagerie professionnelle doit être préfixé dans l'objet par « privé » ou « personnel » et être classés dès l'envoi dans un dossier lui-même dénommé « privé » ou « personnel ». Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé « privé » ou « personnel ». En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel. Ces règles sont également recommandées lors d'un échange avec une institution représentative du personnel ;
- L'utilisation à titre privé d'internet est fortement recommandée sur les temps de pause pour ne pas bloquer ou ralentir le réseau informatique ;
- L'utilisation à titre privé du téléphone fixe est fortement recommandée sur les temps de pause pour ne pas bloquer la ligne téléphonique ;
- Les documents personnels ne doivent pas être inclus dans la sauvegarde professionnelle de la commune (Exemple : pas de stockage de document personnel sur les lecteurs réseaux) ;
- En cas de départ définitif de la commune, l'utilisateur doit prendre les dispositions nécessaires pour ne plus recevoir de messages à titre privé sur sa messagerie professionnelle et également veiller à ce qu'il n'y ait plus de messages à titre privé sur cette dernière.

Pour des raisons de sécurité, est également considéré comme faisant partie du système d'information et de communication, le matériel informatique personnel des salariés connecté au réseau de la commune, ou contenant des informations à caractère professionnel concernant la commune. Les règles définies dans le paragraphe *2.1.2 Appartenant à la* peuvent donc s'y appliquer.

Il est rappelé que la commune met à disposition une adresse électronique nominative. L'aspect nominatif de l'adresse électronique constitue un simple prolongement de l'adresse administrative et ne retire en rien le caractère professionnel de la messagerie.

2.1.5 Pour le travail à distance

Lorsque la commune a mis en œuvre le travail à distance, l'utilisateur peut accéder aux données de la commune à distance. Si elle n'est pas assez sécurisée, cette pratique peut fragiliser l'ensemble du système informatique de la commune.

Bien que géographiquement éloigné des locaux de la commune, l'utilisateur reste responsable des données qu'il manipule et de leur sécurité. Il doit donc appliquer les bonnes pratiques du présent document (cf. *2.1 Du matériel informatique et des logiciels*) sur son lieu de travail à distance.

2.2 D'internet

Internet est un réseau informatique accessible à tout public et fournissant des services divers et variés. A ce titre, une mauvaise utilisation d'internet peut représenter un risque pour la commune. Lorsqu'il navigue sur internet, l'utilisateur doit prendre toutes les précautions utiles pour veiller à la protection des données et des missions de la commune. De ce fait, il se doit de :

- Ne pas utiliser des services de vidéo, de musique et de radio en ligne en dehors de la stricte nécessité de ses fonctions au sein de la commune. En effet, l'utilisation de ces services nécessite des ressources matérielles conséquentes pouvant occasionner des ralentissements sur le réseau informatique de la commune. Les ralentissements du réseau auront des répercussions sur la réalisation de vos missions ou celles de vos collègues ;
- Ne pas télécharger de contenus volumineux. Le téléchargement de contenus volumineux peut avoir les même répercutions que l'utilisation de services de consultation vidéo ou d'écoute de musique/radio en ligne ;
- Ne pas télécharger des logiciels n'ayant aucun lien avec ses fonctions et ses activités professionnelles. Les logiciels peuvent véhiculer des logiciels malveillants ;
- Ne pas consulter des sites internet dont le contenu est contraire à la réglementation en vigueur mais également aux bonnes mœurs de la commune (média à caractère pornographique, …) ;
- Ne pas porter atteinte aux intérêts de la commune ;
- Etre vigilant lors de sa navigation sur internet. Un site internet peut véhiculer des logiciels malveillants. L'utilisateur doit donc en cas de suspicion se rapporter au paragraphe *3.7 Devoir de signalement et d'alerte ;*
- Ne pas cacher son identité sur internet ;
- Ne pas contourner les dispositifs de protection pour accéder à internet (cf. *4.2 Mesures de sécurité mises en œuvre*).

2.3 Pour la continuité d'activité

Pour permettre à la commune de garantir la continuité de ses missions, l'utilisateur doit au quotidien faciliter la potentielle reprise de ses missions par un autre utilisateur.

Pour cela, il doit documenter ses actions, organiser et classer les documents qu'il manipule, de manière suffisamment compréhensible par un autre utilisateur.

En cas d'absence, l'utilisateur doit :

- Veiller à ce que les documents, les logiciels et les dossiers indispensables à l'exercice de son activité soient accessibles par son supérieur hiérarchique ou par la personne désignée pour reprendre son activité ;
- S'assurer qu'un message d'absence a été mis en place en indiquant la date de la fin de l'absence lorsqu'elle est connue et en signalant l'adresse email à contacter en cas de nécessité.

En cas d'absence d'un utilisateur et seulement lorsque le bon fonctionnement du service l'exige, la ou les personnes en charge de l'informatique peuvent :

- Positionner un message d'absence sur la messagerie de l'utilisateur absent ;
- Transférer ponctuellement au supérieur hiérarchique, à sa demande formelle, des emails à caractère exclusivement professionnel présents sur la messagerie de l'utilisateur absent. Ce dernier est informé, dès que possible, de la liste des emails qui

ont été transférés. Le travail de la personne ou les personnes en charge de l'informatique sera facilité si l'utilisateur a respecté la règle de tri des messages personnels (cf. *2.1.4 A des fins privées*) ;
- Transmettre ponctuellement au supérieur hiérarchique, à sa demande formelle, des documents à caractère exclusivement professionnel stockés sur le matériel informatique de l'utilisateur absent. Ce dernier est informé, dès que possible, des documents transmis.

En cas de départ définitif, pour éviter que des emails ne soient pas relevés, l'utilisateur respecte la procédure suivante :

- L'utilisateur envoie un message à ses correspondants habituels en leur indiquant la date de son départ et en leur signalant l'adresse email à laquelle ils devront envoyer leurs messages à partir de cette date au titre des fonctions qu'il quitte ;
- Juste avant son départ, l'utilisateur enregistre dans un fichier les messages qu'il doit transmettre à son successeur et remet ce fichier à son supérieur hiérarchique.

En cas d'absence prolongée ou de départ définitif d'un utilisateur, le supérieur hiérarchique peut demander à la personne responsable en charge de l'informatique, après accord du Maire, l'accès à la messagerie électronique de l'utilisateur. La demande sera formalisée.

2.4 Pour les échanges : Email, tchat, visio, …

L'utilisateur est amené dans le cadre de ses missions à échanger des informations par différents moyens de télécommunication (Email, tchat, réseaux sociaux, ….). Il doit être vigilant avant l'envoi de ces messages et notamment :

- Vérifier l'identité du ou des destinataires concernés par ces messages ;
- S'assurer que les informations diffusées, peuvent être portées à la connaissance du ou des destinataires ;
- Respecter la réglementation et les bonnes pratiques de la communication en général ;
- Ne pas engager indûment la commune, notamment lorsque le contenu du message implique le visa de l'autorité territoriale ;
- Partager (indirectement ou directement) des informations à caractère personnel, concernant des individus et notamment leur vie privée uniquement dans le cadre réglementaire sur la protection des données à caractère personnel ;
- Sur l'historique des messages lorsqu'il effectue un transfert ou un partage.

2.4.1 Email

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée (Cci) pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

Le risque de retard, de non remise et de suppression automatique des messages doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants sont envoyés avec un accusé de réception. Ils doivent le cas échéant, être doublés par des envois postaux.

L'utilisateur se rapprochera de la ou les personnes en charge de l'informatique s'il souhaite connaître la solution qui lui permettrait d'envoyer des fichiers volumineux. Même si des services en ligne gratuits permettent l'envoi de documents volumineux, l'utilisateur

ne peut les utiliser sans l'autorisation expresse de la personne en charge de l'informatique (cf. *2.1.2 N'appartenant pas à la commune)* et que si la commune dispose d'un lien contractuel avec la société qui délivre ce service.

2.4.2 Réseaux sociaux

Les médias sociaux regroupent tous les sites internet, applications ou plateformes qui permettent aux utilisateurs de créer du contenu, de l'organiser, de le modifier ou de le commenter. Les plateformes sociales sont des véritables espaces publics, visibles et consultables par tous.

Ainsi, la communication institutionnelle sur les réseaux sociaux n'est possible que dans le cadre des missions de l'utilisateur définies par la commune et après autorisation expresse de la hiérarchie.

Les moyens d'accès aux différents comptes des réseaux sociaux de la commune doivent obligatoirement se faire sous la responsabilité d'un agent de la mairie afin de garantir la continuité éditoriale de la commune.

Tout ce que l'utilisateur publie ou retransmet (partage, "like", retweet, commentaire, etc.) l'implique personnellement.

2.4.3 Conservation

Les messages échangés par les utilisateurs occupent un espace non négligeable sur les espaces de stockage. Afin d'éviter de surcharger ces espaces, l'utilisateur doit respecter les règles suivantes :

- Conserver tous les messages envoyés ou reçus qui peuvent avoir une valeur probatoire ;
- Lorsque c'est possible, détacher les pièces jointes et les enregistrer ;
- Sauvegarder régulièrement les messages obsolètes et importants. Par exemple, l'utilisateur peut sauvegarder l'année N-2 une fois par an ;
- Supprimer rapidement tous les messages volumineux et sans valeur contractuelle.

3 PROTECTION DES INFORMATIONS

3.1 Confidentialité

Les informations produites par la commune peuvent parfois être confidentielles pour le public mais également pour les collègues. Il est demandé à ce que les utilisateurs soient vigilants sur l'accès aux données tant papier que numérique. Des précautions élémentaires peuvent être prises :

- En enfermant les supports de stockage nomades lorsqu'ils ne sont pas utilisés ;
- En dissimulant les documents papier (feuilles retournées, dossier fermé, …) lorsqu'elles ne sont pas utilisés ;
- En veillant à ce que les documents papiers contenant des informations sensibles (financière, médicale, …) ou nominatives (nom, adresses, photos de personnes…) ne soient pas accessibles à des personnes non autorisées (conservation sous clés, …) ;
- En récupérant les documents dès la fin de l'impression. Cette mesure est à prendre en compte lorsque la ou les imprimantes sont accessibles à d'autres utilisateurs.

Lorsqu'un utilisateur constate qu'il peut accéder à des informations dont il ne devrait pas avoir connaissance, il doit en informer au plus tôt sa hiérarchie et/ou l'utilisateur en charge de ces informations.

Tout support (papier, clé USB…) comportant des informations sensibles ou nominatives doit être rendu illisible avant mise au rebut.

3.2 Données à caractère personnel

La législation européenne (Règlement Général de Protection des Données Personnelles - RGPD) et la loi française (loi Informatique et Libertés de 1978 modifiée par le RGPD) imposent aux entreprises comme aux acteurs publics un cadre qui protège de manière renforcée les données personnelles des Européens.

La commune applique ces règles pour ses propres services et veille également à leur respect par les entreprises qui travaillent pour son compte. Afin de garantir le niveau le plus élevé de protection des données des citoyens, la commune intègre des clauses de protection des données personnelles dans ses marchés publics comme dans ses contrats dès lors que les projets soutenus impliquent la collecte et le traitement de données personnelles.

Un traitement est une ou des opérations, portant sur des données personnelles.

3.2.1 Droit d'accès individuel aux données

Chaque utilisateur peut demander à consulter les données qui le concerne et que détient la commune et à en obtenir communication. Les demandes doivent être adressées par écrit auprès du Délégué à la Protection des Données :

dpd-mutualises@lillemetropole.fr

3.2.2 Création et modification d'un traitement

Lorsque l'utilisateur crée un nouveau traitement ou modifie un traitement déjà existant et comportant des données personnelles, il doit en informer sa hiérarchie, la ou les personnes en charge de l'informatique le cas échéant et le Délégué à la Protection des Données.

3.2.3 Relation contractuelle avec tiers

Lorsque la création ou la modification d'un contrat, d'un marché ou d'une convention avec un tiers (sous-traitant, association, prestataire, partenaire, …) concerne des données à caractère personnel, l'utilisateur doit informer sa hiérarchie, la ou les personnes en charge de l'informatique le cas échéant et le Délégué à la Protection des Données.

En effet, des clauses contractuelles spécifiques à la protection des données doivent être présentes dans le contrat, la convention ou le marché concerné. Ces clauses doivent notamment prévoir des fonctionnalités qui permettent l'exercice des droits de chacun.

3.2.4 Violation de données

On entend par violation de données tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant un impact sur des données personnelles.

Si l'utilisateur constate une violation de données, il alerte sa hiérarchie, la ou les personnes en charge de l'informatique et le service RGPD mutualisé dans les plus brefs délais. L'utilisateur met en œuvre toutes les précautions décrites dans la présente charte.

3.2.5 Durée de conservation

Lorsqu'il est mis fin à un traitement contenant des données à caractère personnel ou lorsque la durée de conservation réglementaire est parvenue à son terme échu, il convient de trier les données (*3.5 Archivage*).

Il est possible de conserver les données à caractère personnel au-delà de la durée de conservation initiale dans le cadre de l'archivage « à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ».

3.3 Mot de passe

L'accès à certains éléments matériels informatiques ou logiciels (comme l'ordinateur, la messagerie électronique, le répondeur, les logiciels métiers ou services en ligne) est protégé par des codes d'accès (par exemple un identifiant et un mot de passe). Ces codes d'accès constituent une mesure de sécurité importante. Ceux-ci visent notamment à protéger les données de toute utilisation malveillante ou abusive. Afin d'en garantir leur efficacité, il appartient à l'utilisateur de :

- Garder les codes d'accès confidentiels. Ils ne doivent pas être communiqués à un autre utilisateur. S'ils ont été notés, ils ne doivent en aucun cas être accessibles à autrui (tiroir fermé à clef, coffre-fort, …) ;
- Ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître. Dans certaines situations, ce fonctionnement n'est pas possible techniquement ou est contraire à la nécessité de continuité d'activité. Ces situations exceptionnelles doivent être encadrées et validées par la hiérarchie. Dans la mesure du possible, elles doivent être corrigées au plus tôt ;
- Ne pas utiliser de mots de passe communs à plusieurs personnes. Néanmoins, cette disposition ne peut pas systématiquement s'appliquer lorsque les comptes ou les ordinateurs sont liés à une fonction commune (email du secrétariat, …). Ces situations exceptionnelles doivent être encadrées et validées par la hiérarchie. Dans la mesure du possible, elles doivent être corrigées au plus tôt ;
- S'assurer que ces mots de passe aient un niveau de complexité suffisant. Pour cela, un mot de passe doit être constitué de 8 caractères au minimum, 12 caractères ou plus dans l'idéal. Ces caractères doivent être un mélange de majuscules, de minuscules, de chiffres et de caractères spéciaux. Certains systèmes ne permettent pas d'appliquer la totalité de ces bonnes pratiques. L'utilisateur essayera donc de rendre son mot de passe le plus robuste possible. Plus le mot de passe est robuste, plus sa découverte par un tiers est difficile ;
- Changer régulièrement (au moins une fois par an) ces mots de passe en évitant de reprendre ceux qui ont déjà été utilisés ;
- Utiliser des mots de passe différents pour chaque accès ;
- Retenir ou stocker ces mots de passe dans un coffre-fort numérique de mots de passe ;
- Ne pas enregistrés ou conservés les mots de passe par les logiciels ou les sites web : ne jamais cocher les cases telles que « se souvenir du mot de passe » ;
- Utiliser la double authentification lorsqu'elle est disponible.

Ces règles peuvent être appliquées grâce à la mise en œuvre de bonnes pratiques. Des informations sur ce sujet sont facilement accessibles sur les sites internet de la CNIL (Commission Nationale Informatique et Liberté) www.cnil.fr et de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) www.ssi.gouv.fr.

3.4 Sauvegarde

La sauvegarde est l'unique solution efficace pour s'affranchir d'une perte de données. L'utilisateur est un des acteurs de l'efficience des sauvegardes. En effet, seul l'utilisateur est en mesure de savoir quelles données à sauvegarder sont nécessaires à l'exécution de ses missions. A ce titre, il doit :

- Identifier, avec la ou les personnes en charge de l'informatique, les données à sauvegarder (données métiers, messagerie, …) et s'assurer qu'elles sont intégrées au dispositif de sauvegarde ;
- Informer la ou les personnes en charge de l'informatique lorsque de nouvelles données essentielles sont à sauvegarder ;
- Utiliser les partages réseaux, lorsqu'ils existent, comme répertoire de travail. Il est déconseillé de travailler sur des documents stockés en local (accessibles sur le Bureau, Mes documents, …) s'ils ne sont pas sauvegardés.

3.5 Archivage

Lorsqu'un utilisateur produit ou reçoit dans le cadre de ses missions et activités pour le compte de la commune, une information qu'elle soit écrite, visuelle ou sonore, sous forme papier ou électronique, ce document est dès lors considéré comme un document d'archives publiques.

Les autres documents non produits par la commune (ex : manuels d'utilisation, guides méthodologiques, revues, textes réglementaires, plaquettes ou brochures d'information) peuvent être éliminés sans passer par la procédure d'archivage lorsqu'ils ne sont plus nécessaires à l'objectif poursuivi. Un tri régulier sur cette documentation obsolète permettra, notamment :

- De concentrer les efforts de classement et de conservation sur les documents d'archives essentiels à l'activité ;
- De faciliter la gestion et de réduire les coûts du stockage des serveurs et de la sauvegarde.

La responsabilité de la conservation des archives produites et reçues par la commune relève de chaque utilisateur. Sur les données et documents numériques, l'archivage électronique permet de pérenniser les données, notamment sur des durées longues, voire de manière définitive.

En tant qu'acteur dans le cycle de vie de la donnée, chaque utilisateur joue un rôle important dans l'archivage et doit donc veiller à :

- Permettre l'accès aux données pendant la durée nécessaire à la réalisation de l'objectif poursuivi par la mission (établissement d'un acte d'état civil, gestion d'un bénéficiaire d'une prestation, inscription aux activités périscolaires, etc.). Cette durée est appelée Durée d'Utilité Courante (DUC) ;
- Vérifier la complétude et la fiabilité des données à conserver : pour les données à caractère personnel, à la fin de la DUC, leur accès doit être restreint. Il est recommandé de les placer dans une base d'archivage intermédiaire avec un accès restreint (ex : classeur rangé dans une armoire d'archivage fermée à clé ou, dans une application informatique spécifique, une base distincte, avec un accès restreint. Les données sont ainsi conservées pendant toute leur Durée d'Utilité Administrative (DUA) ;

- Conserver uniquement, à la fin de la DUA, les données nécessaires, à savoir les données qui permettent de satisfaire l'objectif poursuivi par l'archivage historique (ou définitif). Détruire les archives non historiques, après obtention d'une autorisation de l'État (procédure d'élimination des archives publiques soumise au visa du directeur des Archives départementales du Nord). À ce titre l'utilisateur peut se référer aux instructions de l'Etat en matière de tri et de conservation des archives publiques, en particulier, les instructions DAF/DPACI/RES/2009/018 du 28 août 2009 et DAF/DPACI/RES/2014/006 du 22 septembre 2014.

Pour l'aider dans cette démarche, l'utilisateur peut se référer aux Archives départementale du Nord ou au service/référent de l'archivage au sein de sa commune.

Lorsqu'il a été mis en place, l'utilisateur suivra le processus organisationnel d'archivage réalisé en interne par la commune ou pourra recourir à un accompagnement ou intervention du Centre de Gestion de la Fonction Publique Territoriale du Nord. Ce processus permet notamment la continuité d'activité des services communaux : savoir quoi conserver, combien de temps, comment, avec quelles restrictions d'accès… Pour permettre une pérennité des données patrimoniales historiques et faciliter les recherches dans les archives, l'utilisateur doit :

- Identifier les données et documents à conserver à long terme (à minima les contenus à conserver plus de 10 ans), indépendamment de la date et de la nature des données ou documents ;
- Classer et nommer à minima ces contenus de manière intelligible ;
- Stocker ces contenus sur les partages réseaux lorsqu'ils existent et les inscrire dans la liste des données à archiver ;
- Privilégier une conservation dans des formats interopérables (formats ouverts et non propriétaires ; pdf, xml, odf, jpeg, tiff, mp3 ou mpeg4, etc. - cf. Référentiel Général d'Interopérabilité).

Lorsque l'utilisateur souhaite acquérir un logiciel informatique, il doit s'assurer au préalable que les clauses contractuelles spécifiques à l'archivage sont présentes dans le contrat ou le marché concerné. Ces clauses doivent notamment prévoir une purge des données et une fonctionnalité d'export conforme au standard d'échange de données pour l'archivage.

3.6 Email non-sollicités

L'Email est le premier vecteur de propagation des virus et de piratage informatique. Il est impossible de garantir au niveau informatique une sécurité totale des Emails. La prévention et la vigilance sont donc les clés de la protection de la commune.

Il existe 4 principales formes d'Email non sollicités qui peuvent être malveillants :

- Les Email d'hameçonnage (Phishing en anglais) : sollicitations frauduleuses d'extorsion de mot de passe (ou autre information personnelle sensible telle que le numéro de carte bancaire) par messagerie ou via un site web contrefait ;
- Les Email publicitaires appelés "SPAM" : il s'agit principalement de messages publicitaires reçus de manière répétée ;
- Les Email canulars appelés "hoax" (anglais) : fausses alertes aux virus, fausses chaînes de solidarité, fausses promesses, fausses informations ;
- Les Email malveillants : ils ont pour objectif d'infecter votre ordinateur et les ordinateurs présents dans la commune, ils peuvent être reçus sous la forme de

l'identité d'un contact connu (service client, fournisseur, partenaire de la commune, ...).

Ces messages peuvent aussi reprendre une conversation que vous avez déjà eu avec un de vos contacts (exemple: " RE : Note de service xxx") afin de vous duper.
Ils peuvent contenir une ou plusieurs pièces jointes infectées (Word, Excel, PDF, …), et plus rarement des liens pointant vers des sites internet compromis ou vers des documents téléchargeables.

Ce type d'Email présente très souvent un caractère urgent.

Les Email non-sollicités surchargent votre messagerie électronique et occupent de la place inutilement lors de la sauvegarde de celle-ci. Ils peuvent aussi présenter un risque de sécurité en infectant le système d'information de la commune.

De ce fait, l'utilisateur :

- Ne doit pas transférer les Email non-sollicités ;
- Doit supprimer les Email non-sollicités ;
- Ne doit pas communiquer ses codes de connexion (login, mot de passe, …) en répondant à une demande par Email ;
- Doit se désinscrire des Email non-sollicités en cliquant sur le lien présent dans le bas du message (« me désinscrire » ou « unsuscribe me »). Dans tous les cas, l'utilisateur ne doit pas fournir d'informations le concernant (login, mot de passe, nom, ...) pour se désinscrire ;
- Ne doit pas ouvrir les pièces jointes lorsqu'il suppose que l'Email est malveillant. Un ordinateur ne peut pas être infecté si la pièce jointe malveillante n'est pas ouverte.

3.7 Devoir de signalement et d'alerte

L'utilisateur doit signaler, dans les plus brefs délais, à la personne ou aux personnes en charge de l'informatique et/ou à sa hiérarchie le cas échéant :

- Tout accès illégitime, tentative d'intrusion et dysfonctionnements anormaux sur son poste de travail, sur ses fichiers ou sur ses logiciels ;
- La présence de fichiers pouvant engendrer un risque pour la sécurité de la commune (fichier vérolé, fichier illicite comme des logiciels pirates, …) ;
- Une réponse par erreur à un email non sollicité (*cf. 3.6 Email non-sollicités*) ;
- La présence de fichier sous droit d'auteur non acquis par la commune ;
- La visualisation d'un message d'alerte du logiciel antivirus ;
- La visualisation d'un message demandant la mise à jour des logiciels. En principe, la mise à jour des logiciels se réalise automatiquement sans l'intervention de l'utilisateur. Dans le cas contraire, la ou les personnes en charge de l'informatique pourront corriger ce problème ;
- La perte ou le vol de matériel informatique appartenant à la commune.

Cela permettra de prendre les mesures sécurités adaptées au plus tôt.

Si un utilisateur constate qu'un ou plusieurs de ses mots de passe sont connus par un autre utilisateur, il doit alors les changer sans délai, et en informer sa hiérarchie. En informant sa hiérarchie, l'utilisateur évite tout contentieux en cas de manipulation frauduleuse de ses accès.

4 GESTION DES SYSTÈMES ET DES RÉSEAUX INFORMATIQUES

4.1 Personne en charge de l'informatique

La ou les personnes en charge de l'informatique sont responsables du contrôle du bon fonctionnement du système d'information et de communication. De ce fait, ils sont :

- En mesure de connaître la bonne application de la présente charte par les utilisateurs ;
- Assujettis à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître ;
- En mesure de prendre les actions nécessaires pour arrêter ou limiter un incident de sécurité.

Lorsqu'une ou des personnes sont en charge de l'informatique dans une commune, elles peuvent fournir à l'utilisateur toute information concernant l'utilisation des matériels informatiques et des logiciels, sur l'évolution des limites techniques et de la surveillance des activités.

4.2 Mesures de sécurité mises en œuvre

L'utilisateur est informé que la commune peut mettre en place des dispositifs de limitation technique sur le matériel informatique et les logiciels de la commune. Ces dispositifs visent uniquement à améliorer techniquement la sécurité. Ces dispositifs peuvent être :

- Un filtrage des sites internet : ce dispositif permet d'interdire l'accès à certaines catégories de sites non autorisées par la présente charte ou par la réglementation en vigueur. L'utilisateur est informé que ce type de dispositif ne permet pas de garantir une efficacité totale ;
- Une limitation liée à l'installation de logiciels : ce dispositif bloque l'installation de logiciels sur les ordinateurs de la commune ;
- Un ou des dispositifs de lutte contre les logiciels malveillants (anti-virus) ;
- Un ou des dispositifs de filtrage de la messagerie (anti-spam, …). L'utilisateur est informé que ce type de dispositif ne permet pas de garantir une efficacité totale.

4.3 Prise en main à distance

La ou les personnes en charge de l'informatique peuvent disposer d'outils de prise en main à distance pour dépanner techniquement les utilisateurs, en leur montrant directement les manipulations à faire.

Ces prises en mains à distance se feront toujours avec l'accord préalable de l'intéressé.

4.4 Surveillance des activités

L'utilisateur est informé que la commune peut mettre en place des dispositifs de surveillance sur l'utilisation du matériel informatique et des logiciels. Ces dispositifs visent à garder un historique de l'utilisation du matériel informatique et des logiciels uniquement pour résoudre des dysfonctionnements techniques, pour la maintenance et l'évolution des matériels informatiques et des logiciels, ou pour identifier les causes d'un incident de sécurité.

Ces dispositifs ne peuvent en aucun cas être utilisés pour surveiller les utilisateurs. La ou les personnes de l'informatique sont les garants de la confidentialité des données manipulées par les dispositifs de surveillance (*cf. 4.1 Personne en charge de l'informatique*). Ces données sont conservées pour une durée maximale de 1 an.

Ces dispositifs peuvent permettre de conserver l'historique de l'activité des utilisateurs de la commune :

- Sur internet (le contenu des sites internet n'est pas conservé) ;
- Sur leur poste bureautique (le contenu des fichiers n'est pas conservé) ;
- Sur les serveurs de partage de fichiers (le contenu des fichiers n'est pas conservé);
- Sur les applications métier ou services en ligne ;
- Sur la ou les messageries (le contenu des messages n'est pas conservé).

D'une manière générale, les caractéristiques des activités historisées sont l'identifiant de l'utilisateur à l'origine de l'activité, l'horodatage de l'activité, l'élément concerné (ex : adresse du site internet accédé, nom du fichier modifié, …) et l'action réalisée (lecture, modification, suppression).