COMMUNE DE

SAINT-PANTALEON-DE-LARCHE

CHARTE
DU SYSTÈME D'INFORMATION

Dispositions applicables dans les services de la commune de Saint Pantaléon-de-Larche

Accusé de réception en préfecture
019-211922901-20240523-DL2024_045-DE
Date de télétransmission : 27/05/2024
Date de réception préfecture : 27/05/2024

1 – Introduction

La présente charte informatique est un code de déontologie formalisant les règles légales et de sécurité relatives à l'utilisation de tout système d'information et de communication au sein de la collectivité et des établissements mentionnés ci-dessous dans le cadre d'une convention ou de la mise à disposition de moyens :

- Commune de Saint Pantaléon-de-Larche

Les différents outils technologiques utilisés offrent au personnel des collectivités une grande ouverture vers l'extérieur. Cette ouverture peut apporter des améliorations de performances importantes si l'utilisation de ces outils technologiques est faite à bon escient et selon certaines règles.
À l'inverse, une mauvaise utilisation de ces outils peut avoir des conséquences extrêmement graves.
En effet, ils augmentent les risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité, d'atteinte à l'intégrité et à la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vols de données).
L'application des nouvelles technologies informatiques et de communication permet de préserver le système d'information, le bon fonctionnement des services et les droits et libertés de chacun. Les chartes sont trop souvent considérées comme un moyen de contrôle du travail des agents. Elles doivent être expliquées aux agents.
La présente charte s'applique à l'ensemble des agents, tous statuts confondus, ainsi qu'au personnel temporaire et aux élus. Elle s'applique également à tout prestataire extérieur ayant accès au système d'information de la collectivité. Tout contrat avec un prestataire extérieur devra faire référence et comporter comme annexe la présente charte.
Dès l'entrée en vigueur de la présente charte, chaque agent de la collectivité s'en verra remettre un exemplaire. Il devra en prendre connaissance et devra s'engager à la respecter.
Le manquement à la présente charte pourra entraîner le retrait du droit d'utilisation d'un outil, d'une application ou d'un matériel informatique/téléphonique et/ou des mesures d'ordre disciplinaire et/ou des sanctions pénales.
Cette charte tient lieu de règlement :

- Référence CM
- Référence avis du CTP

2 - Définitions

Système d'information : un système d'information, généralement abrégé « SI » est un ensemble organisé de ressources permettant de collecter, regrouper, classifier, traiter et diffuser de l'information dans un environnement donné. Ces ressources peuvent être de plusieurs types : matériel, logiciel, personnel, données et procédures, services en ligne, échanges et communications électroniques, etc.
La notion de système d'information est donc plus vaste que le domaine des logiciels informatiques, contrairement à certaines idées reçues : les logiciels et outils informatiques ne sont qu'une des composantes des systèmes d'information.
Important : les dispositions du règlement européen sur la protection des données (RGPD) et de la loi française s'appliquent également aux données et traitements réalisés manuellement sur la base de documents papier (formulaires, fiches, registres, etc.).

Ressources informatiques : désigne globalement les moyens informatiques de calcul ou de gestion locaux ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par la commune.

Services Internet : désigne la mise à disposition, par des serveurs locaux ou distants, de moyens d'échanges ou d'informations divers : Web, navigation Internet, messagerie, forums, réseaux sociaux, serveurs d'échanges, services en ligne, stockage distant (Cloud), systèmes permettant l'organisation et la réalisation d'échanges, réunions, formations via audioconférence ou visioconférence…

Utilisateur : désigne les personnes ayant accès ou utilisant les ressources informatiques et services Internet, quels que soient les droits attribués.

RGPD : règlement européen sur la protection des données. Il vise à harmoniser et renforcer la protection des données personnelles en définissant un cadre juridique, avec trois objectifs : renforcer les droits des personnes, responsabiliser les acteurs traitant des données, crédibiliser la régulation

Accusé de réception en préfecture
019-211922901-20240523-DL2024_045-DE
Date de télétransmission : 27/05/2024
Date de réception préfecture : 27/05/2024

grâce à une coopération renforcée entre les autorités de protection des données. Les dispositions du règlement européen (2016/679) prévalent sur la loi française.

Responsable de traitement : désigne la personne, l'autorité publique, la société ou l'organisme qui détermine les finalités et les moyens de ce fichier, qui décide de sa création. En pratique, il s'agit généralement de la personne morale (entreprise, collectivité, etc.) incarnée par son représentant légal (président, maire, etc.).

Délégué à la protection des données (DPO) : désigne la personne chargée de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme. Le délégué peut être interne ou externe.

Donnée personnelle : désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou non, grâce à un identifiant ou à un ou plusieurs éléments propres à son identité.

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

3 - Règles générales d'utilisation

Les utilisateurs sont supposés adopter un comportement responsable s'interdisant par exemple toute tentative d'accès à des données ou à des sites qui leur seraient interdits.
Tout utilisateur est responsable des usages qu'il fait des ressources du système d'information, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau.
Il doit en permanence garder à l'esprit que c'est sous le nom de la collectivité qu'il se présente sur Internet et dans les échanges électroniques et doit se porter garant de l'image de l'institution.
Au même titre que pour les documents papier ou le téléphone, chacun est responsable des messages envoyés ou reçus, et doit utiliser le système d'information dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues et des règles élémentaires de courtoisie et de bienséance.

4 - Droits et devoirs des utilisateurs

Toute personne (agent titulaire, contractuel, stagiaire) travaillant ou titulaire d'un mandat (élu) dans la collectivité ou personne externe intervenant dans le cadre d'un contrat pour la collectivité peut disposer, pour l'exécution de ses missions, d'un droit d'accès au système d'information.
Ce droit d'accès est strictement personnel et incessible.
Les ressources du système d'information mises à disposition constituent un outil de travail nécessaire.
Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l'utilisation des ressources et notamment :

- Prendre connaissance des informations diffusées par la collectivité et les appliquer en permanence dans l'exécution des tâches et missions confiées ;
- Respecter l'intégrité et la confidentialité des données et ne pas perturber la disponibilité du système d'information ;
- Ne pas rechercher, consulter, stocker ou transmettre d'informations portant atteinte à la dignité humaine ;
- S'interdire de marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée ;
- Informer l'autorité territoriale préalablement à la mise en œuvre d'une collecte ou d'un traitement contenant des données à caractère personnel et déclarer ceux en place à l'entrée en vigueur de la présente charte ;
- Respecter le droit de propriété intellectuelle : non-reproduction et/ou non-diffusion de données soumises à un droit de copie non détenu, interdiction de copie de logiciel sans licence d'utilisation ;

Accusé de réception en préfecture
019-211922901-20240523-DL2024_045-DE
Date de télétransmission : 27/05/2024
Date de réception préfecture : 27/05/2024

- Ne pas porter atteinte à la sécurité du système d'information par l'utilisation de ressources extérieures matérielles ou logicielles ;
- Respecter les contraintes liées à la maintenance du système d'information.

5 - Droits et devoirs de la collectivité

La conformité au règlement européen sur la protection des données (RGPD)

Le règlement européen sur la protection des données, applicable depuis le 25 mai 2018, renforce encore les obligations en matière de transparence des traitements et de respect des droits des personnes. Il s'axe sur une logique globale de responsabilisation de l'ensemble des acteurs et crédibilise la régulation des « CNIL » en musclant considérablement leur pouvoir de sanction.

Ainsi, outre des avertissements publics, elles pourront prononcer des amendes.

Le règlement européen sur la protection des données introduit pour les collectivités territoriales une logique de responsabilisation.

Si les grands principes déjà présents dans la loi Informatique et Libertés ne changent pas, un véritable changement de culture s'opère. On passe en effet d'une logique de contrôle *a priori* basé sur des formalités administratives (déclaration) à une logique de responsabilisation des acteurs privés et publics.

Ce changement de posture se traduit par une mise en conformité permanente et dynamique de la part des collectivités qui ont obligation d'adopter et actualiser des mesures techniques et organisationnelles leur permettant de s'assurer et de démontrer à tout instant qu'elles offrent un niveau optimal de protection aux données traitées.

Les organismes publics et privés auxquels les collectivités sous-traitent la mise en œuvre de tout ou partie de leurs traitements (ex. : prestataires de service hébergeant des données) doivent obligatoirement participer à la démarche de mise en conformité, en aidant celles-ci à satisfaire leurs diverses obligations, sous peine de sanctions.

Les collectivités doivent intégrer un nouveau principe de protection des données dès la conception (Privacy by design) du traitement et par défaut (Privacy by default).

Elles doivent ainsi tenir compte le plus en amont possible, dès la phase de conception du produit, du service ou du traitement, de définition des outils qui seront utilisés et des paramétrages par défaut, des règles d'or de la protection des données. Il s'agit en particulier de minimiser à tout point de vue le traitement effectué.

Quelques exemples :

- Favoriser par principe les menus déroulants ou les cases à cocher plutôt que les zones de commentaires libres sur les formulaires de collecte et dans les bases de données, pour limiter dès le départ le nombre et la nature des données enregistrées ;
- Restreindre au maximum les droits d'accès informatiques aux données et les opérations susceptibles d'être réalisées ;
- Pseudonymiser les données toutes les fois où leur exploitation sous une forme identifiante n'apparaît pas nécessaire à la satisfaction du besoin ;
- Appliquer un mécanisme automatique de purge des données à l'issue de la durée de conservation nécessaire à la réalisation de la finalité.

Avec le règlement, on assiste à un allègement considérable des obligations en matière de formalités préalables, puisque le régime déclaratif est totalement supprimé, pour entrer dans l'ère de la gouvernance des données personnelles. Une bonne gouvernance nécessite toutefois une documentation continue des actions menées pour être en capacité de piloter et de démontrer la conformité. Les collectivités seront ainsi appelées à tenir un registre de leurs activités de traitement, à encadrer les opérations sous-traitées dans les contrats de prestation de services, à formaliser des politiques de confidentialité des données, des procédures relatives à la gestion des demandes d'exercice des droits, à adhérer à des codes de conduite ou encore à certifier des traitements.

Dans certains cas, pour les traitements à risques, elles doivent effectuer une analyse d'impact sur la vie privée et notifier à la CNIL, voire aux personnes concernées, les violations de données personnelles.

Depuis le 25 mai 2018, la désignation d'un délégué à la protection des données (DPO) est obligatoire pour les organismes et autorités publics, et donc pour les collectivités.

Le délégué a pour principales missions :

- Informer et conseiller le responsable de traitement de la collectivité ou le sous-traitant, ainsi que les agents ;
- Diffuser une culture Informatique et Libertés au sein de la collectivité ;
- Contrôler le respect du règlement et du droit national en matière de protection des données, via la réalisation d'audits en particulier ;

Accusé de réception en préfecture
019-211922901-20240523-DL2024_045-DE
Date de télétransmission : 27/05/2024
Date de réception préfecture : 27/05/2024

- Conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- Coopérer avec la CNIL et être le point de contact de celle-ci.

Dans l'exercice de ses missions, le délégué doit être à l'abri des conflits d'intérêts, rendre compte directement au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté certaine dans les actions qu'il décide d'entreprendre.

Information individuelle - La collectivité peut satisfaire à cette obligation par la diffusion de tous documents précisant les règles d'usage de son système d'information ainsi qu'à leur application (charte du système d'information, règlement intérieur, notes de service, documentations spécifiques…). Cette diffusion s'effectue sous forme de documents imprimés ou électroniques.
Le Comité Technique compétent doit être consulté sur le sujet.

Disponibilité et intégrité du système d'information - La collectivité s'engage à :

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

6 – Analyse, contrôle, maintenance

Pour des nécessités légales, de sécurité, de maintenance (ensemble des activités de type curatif, préventif, correctif et évolutif) et de gestion technique, l'utilisation du système d'information peut, sous le contrôle de l'autorité territoriale, être analysée et contrôlée. Pour l'ensemble des outils et matériels, la désactivation, même temporaire, des solutions permettant la réalisation de ces opérations est interdite.
Les outils de télémaintenance sont autorisés et l'utilisateur du système d'information doit être informé préalablement de toute intervention et de la fin de l'intervention. Un rapport d'intervention est enregistré par l'autorité territoriale afin de tracer les opérations réalisées.

7 – Sanctions

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

8 – Évolutions

Avant son entrée en vigueur, la charte est soumise à l'avis du Comité Technique. Elle pourra être complétée ou modifiée par l'autorité territoriale, l'avis du Comité Technique sera à nouveau demandé.

9 – Équipements

- Un équipement = matériels, système d'exploitation, logiciels/applications.
- Toute installation logicielle est à la charge de la personne compétente et désignée par l'autorité territoriale.
- En cas d'absence momentanée, l'utilisateur doit verrouiller l'accès à son équipement. Pour une durée prolongée, l'utilisateur doit également quitter les applications.
- À la fin de sa journée de travail, l'utilisateur doit quitter les applications, arrêter le système par arrêt logiciel, et mettre hors tension l'équipement à sa disposition.

Accusé de réception en préfecture
019-211922901-20240523-DL2024_045-DE
Date de télétransmission : 27/05/2024
Date de réception préfecture : 27/05/2024

- Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tiers et régulièrement modifiés.
- L'utilisateur doit signaler tous dysfonctionnements ou anomalies au service ou référent informatique selon la procédure définie par la collectivité.
- L'utilisateur doit procéder régulièrement à l'élimination des fichiers non utilisés et à l'archivage tel que défini par l'autorité territoriale.
- Les supports amovibles (CD, clés USB, etc.) provenant de l'extérieur doivent être soumis à un contrôle antivirus préalable.

10 – Messagerie

- L'utilisation de la messagerie est réservée à des fins professionnelles. Néanmoins il est toléré en dehors des heures de travail un usage modéré de celle-ci pour des besoins personnels et ponctuels.
- La lecture des courriels personnels reçus durant les heures de travail est tolérée si celle-ci reste occasionnelle.
- L'utilisateur veille à ne pas ouvrir les courriels dont le sujet paraît suspect.
- Tout courrier électronique est réputé professionnel : il est donc susceptible d'être ouvert par l'autorité territoriale ou le référent informatique, ceci même en l'absence de l'utilisateur. Les courriers à caractère privé et personnel doivent expressément porter la mention « personnel et confidentiel » dans leur objet. Ces derniers ne pourront alors être ouverts par l'autorité territoriale ou le référent informatique que pour des raisons exceptionnelles de sauvegarde de la sécurité ou de préservation des risques de manquement de droit des tiers ou à la loi.
- L'utilisateur s'engage à ne pas envoyer en dehors des services de la collectivité des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel et autorisé par sa hiérarchie.
- L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.
- L'utilisateur signe tout courriel professionnel en respectant la charte graphique de la collectivité.
- L'utilisateur vérifie la liste des destinataires et respecte les circuits de l'organisation ou la voie hiérarchique le cas échéant.
- L'utilisateur vérifie le contenu et l'historique des messages transférés (gestion du « Répondre à tous »).
- L'utilisateur évite de surcharger le réseau d'informations inutiles. Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.
- En cas d'absence prévisible, l'utilisateur met en place un message automatique d'absence indiquant la date de retour prévue. Un agent du service doit pouvoir gérer les messages pendant son absence.
- La signature électronique (loi n° 2000-230 du 13 mars 2000) est présumée fiable jusqu'à preuve du contraire. Son utilisation est limitée aux personnes autorisées et doit respecter la procédure définie par la collectivité.
- Une équivalence juridique est établie entre le courrier électronique et le courrier sur support papier (ordonnance n° 2005-1516 du 8 décembre 2005). Ils doivent en conséquence être traités dans les mêmes délais.

11 – Sites Internet

- L'utilisation d'Internet est réservée à des fins professionnelles et/ou syndicales dans le cadre de l'exercice des décharges d'activité et autorisations spéciales d'absence.
- Néanmoins, il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.
- L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine.
- Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.
- Le stockage sur les matériels mis à disposition de données à caractère non professionnel téléchargées sur Internet est interdit.

Accusé de réception en préfecture
019-211922901-20240523-DL2024_045-DE
Date de télétransmission : 27/05/2024
Date de réception préfecture : 27/05/2024

- Tout abonnement payant à un site Web ou à un service via Internet doit faire l'objet d'une autorisation préalable de l'autorité territoriale.
- Pour éviter les abus, l'autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites les plus visités (Cass. soc. 9 juillet 2008 n° 06-45-800).
- Toute saisie d'informations sur un site Internet professionnel nécessite l'autorisation préalable de l'autorité territoriale.
- Toute procédure d'achats personnels sur Internet est formellement interdite.
- L'utilisation de forums de discussion est autorisée pour un usage professionnel.

12 – Réseaux sociaux

- L'utilisation des réseaux sociaux est réservée à des fins professionnelles. Néanmoins il est toléré en dehors des heures de travail un usage modéré pour des besoins personnels et ponctuels.
- La consultation des comptes personnels durant les heures de travail est tolérée si celle-ci reste occasionnelle.
- L'utilisation doit être appropriée et doit respecter le devoir de réserve.
- Des autorisations de communication sur les réseaux sociaux sont attribuées aux agents, aux services qui sont habilités à parler au nom de la collectivité et fixent précisément le modèle de communication décidé.
- La distinction entre l'utilisation professionnelle et l'utilisation personnelle est obligatoire (création de deux profils).
- Les conditions d'utilisation et d'accès sont définies (restrictions et limites pratiques).

13 - Téléphones et équipements mobiles

Règles d'utilisation

- L'utilisation des téléphones fixes et portables est réservée à des fins professionnelles. Néanmoins, un usage ponctuel du téléphone pour des communications personnelles locales est toléré à condition que cela n'entrave pas l'activité professionnelle.
- L'utilisation des téléphones portables personnels doit rester limitée, occasionnelle et discrète (appels, SMS et notifications).
- L'autorité territoriale peut procéder au contrôle de l'ensemble des appels émis à partir des équipements mis à disposition.
- En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique.
- L'agent qui quitte définitivement la collectivité doit restituer le téléphone portable professionnel.
- L'utilisateur doit veiller à soigner sa présentation lors d'un appel pour faciliter son identification et/ou son service.
- L'équipement mobile est un outil de travail dont l'usage personnel peut être autorisé (mention « personnel » pour messages personnels).
- Il n'est pas obligatoire de répondre aux appels, messages, courriels en dehors du temps de travail (soir, week-end et congés) à l'exception des astreintes et situations prévues dans le cadre des missions confiées.
- Les communications disponibles au moyen des équipements mobiles ne doivent pas venir perturber une réunion ou un entretien qui sont des évènements sociaux qui nécessitent la présence physique et intellectuelle de chacun.

14 - Bases légales

L'utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n° 84-53 du 26 janvier 1984 relative à la fonction publique territoriale.
Cette présente partie a pour objectif d'informer les utilisateurs des textes législatifs et réglementaires dans le domaine de la sécurité des systèmes d'information.

Réglementation

- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

- 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.
- Loi nº 2016-1321 du 7 octobre 2016 pour une République numérique.
- Loi nº 2018-493 relative à la protection des données personnelles du 20 juin 2018.
- Loi nº 78-753 du 17/07/1978 sur la liberté d'accès aux documents administratifs.
- Loi nº 85-660 du 03/07/1985 sur les droits d'auteur et la protection des logiciels.
- Loi nº 91-646 du 10/07/1991 relative au secret des correspondances émises par voie de télécommunication.
- Loi nº 2000-230 du 13/03/2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
- Loi nº 2004-575 du 21/06/2004 pour la confiance dans l'économie numérique.
- Loi nº 2012-410 du 27/03/2012 relative à la protection de l'identité.

Droit disciplinaire

- Loi nº 84-53 du 26 janvier 1984 (art. 89 et 90) et le décret nº 89-677 du 18 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux.
- Décret nº 92-1194 du 4 novembre 1992 (art. 6) fixant les dispositions communes applicables aux fonctionnaires stagiaires de la fonction publique territoriale.
- Décret nº 88-145 du 15 février 1988 (art. 36 et 37) relatif aux agents contractuels.
- Décret nº 91-298 du 20 mars 1991 (art. 15) relatif aux agents à temps non complet.

Code pénal

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