Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le 24/06/2025
ID : 048-214801326-20250620-920062025-DE

DELIBERATION DU CONSEIL MUNICIPAL
DE SAINT-ALBAN-SUR-LIMAGNOLE
SEANCE VENDREDI 20 JUIN 2025

CONS	
EN EXERCICE :	15
PRÉSENTS :	10
Procurations :	4
Absente :	1

L'an deux mille vingt-cinq et le vingt juin à vingt heures trente, le Conseil Municipal s'est réuni au nombre prescrit par la loi dans le lieu habituel de ses séances, sous la présidence de Monsieur Samuel SOULIER, Maire de SAINT-ALBAN-SUR-LIMAGNOLE.

Présents : BALMADIER André, BECHETOILLE Xavier, BRUNET Jean-Marie, CHAMPREDON Éric, CONSTANT Sandrine, DOLADILLE Damien, GOEURY Béatrice, PAGES Anne, SOULIER Samuel, TREBUCHON Géraldine.
Présents par procuration : PANTEL BEILLA Emilie à GOEURY Béatrice, PARENT Philippe à DOLADILLE Damien, RODIER Sylvain à BRUNET Jean-Marie, SOULIER Anne à CONSTANT Sandrine.
Absente : Madame DOMEIZEL Emilie
Secrétaire de séance : Madame CONSTANT Sandrine

9 - OBJET : APPROBATION DE LA CHARTE D'UTILISATION DES MOYENS INFORMATIQUES ET DES OUTILS NUMERIQUES

Le Conseil Municipal,
Vu le Code général des collectivités territoriales,
Vu la nécessité de fixer des règles d'usage pour les moyens informatiques et les outils numériques mis à disposition des agents, des usagers et des élus,
Vu le projet de Charte d'utilisation des moyens informatiques et des outils numériques annexé à la présente délibération,
Considérant l'importance de garantir la sécurité des systèmes d'information, le respect des données personnelles, et le bon usage des outils numériques dans le cadre professionnel,

Après en avoir délibéré, le Conseil Municipal décide à l'unanimité :

Article 1 : La Charte d'utilisation des moyens informatiques et des outils numériques annexée à la présente délibération est approuvée.

Article 2 : Cette charte s'applique à l'ensemble des agents / personnels / usagers / élus, utilisant les ressources informatiques de la Commune de Sant Alban sur Limagnole.

Article 3 : Le Maire est chargé de veiller à la diffusion et à la bonne application de cette charte.

Le Maire,

Samuel SOULIER

MAIRIE DE SAINT-ALBAN (Lozère)

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le 24/06/2025
ID : 048-214801326-20250620-920062025-DE

Charte d'utilisation des moyens informatiques et des outils numériques

Délégué à la protection des données : dpd@cdg48.fr

Contact :

SOMMAIRE

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le
ID : 048-214801326-20250620-920062025-DE

INTRODUCTION

Le contexte et les enjeux

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.

A l'inverse, une mauvaise utilisation de ces outils peut entraîner 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).

De plus, mal utilisés, les outils informatiques peuvent aussi être une source de perte de productivité et de coûts additionnels.

L'application des nouvelles technologies informatiques et de communication permettent 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 au personnel.

L'objectif

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.

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.

Le champ d'application

La présente charte s'applique à **l'ensemble du personnel tous statuts confondus, ainsi qu'au personnel temporaire et aux élus**.

Elle s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques 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 (cf. Récépissé).

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le
ID : 048-214801326-20250620-920062025-DE

Chapitre 1 : Règles d'utilisation des ressources

1) Les utilisateurs sont supposés adopter un comportement responsable s'interdisant par exemple toute tentative d'accès à des données ou à des sites qui leurs seraient interdits.

2) Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient entraîner 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 doit se porter garant de l'image de l'institution.

3) Au même titre que pour le courrier papier ou le téléphone, chacun est responsable des messages envoyés ou reçus, et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues et des règles élémentaires de courtoisie et de bienséance.

A - Les droits et les devoirs des utilisateurs

4) Un accès aux ressources réglementé

Toute personne (agent et élu) travaillant dans la collectivité dispose d'un droit d'accès au système d'information. Ce droit d'accès est :

- Strictement personnel.
- Incessible.

5) Une utilisation professionnelle des ressources

Les ressources informatiques 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 :

- Respecter l'intégrité et la confidentialité des données.
- Ne pas perturber la disponibilité du système d'information.
- Ne pas stocker ou transmettre d'informations portant atteinte à la dignité humaine.
- Ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée (loi « informatique et liberté » du 06/01/1978).
- 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.
- 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.

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le
ID : 048-214801326-20250620-920062025-DE

B - Les droits et les devoirs de la collectivité

6) La conformité au RGPD :

Le Règlement 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) est entré en vigueur le 28 mai 2018. Toute collectivité a obligation d'être en conformité avec ce règlement et de désigner un Délégué à la Protection des Données (DPO).

7) L'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 informatique, règlement intérieur, note de service...).

Le Comité Technique compétent doit être consulté sur le sujet.

8) La disponibilité et l'intégrité du système informatique :

La collectivité s'engage à :

- Mettre à disposition les ressources informatiques matérielles et logicielles 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 matériels et des logiciels 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.

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le
ID : 048-214801326-20250620-920062025-DE

Chapitre 2 : Messagerie et agenda électronique

Sous-chapitre 1 : Messagerie électronique

9) Le champ « destinataire » (A :) est réservé aux personnes devant mener une action relative au contenu du mail.
Le champ « copie » (Cc :) est réservé aux personnes destinataires de courriel pour information.
Le champ « copie cachée » (Cci :) est réservé à la protection des données personnelles des destinataires quand il ne faut pas divulguer leur identité.

L'utilisateur doit éviter l'envoi de copies à un nombre injustifié de personnes afin, notamment, de ne pas surcharger le serveur de messagerie.

Tout courrier électronique engageant la collectivité doit respecter les mêmes règles que tout autre courrier. Le courrier électronique constitue un élément de preuve devant la justice.

10) Pour des raisons d'espace de stockage, de performance des systèmes et de sobriété énergétique, la taille des messages est limitée à 8 mo.

Point bilan carbone :
- Un mail sans PJ : 4g de CO2
- Un mail avec une PJ de 1 Mo envoyée à **10 personnes** : 50g de CO2 soit environ **500 mètres en voiture**

Lorsque des pièces volumineuses doivent être partagées en grand nombre, afin de réduire l'impact écologique du transfert, on privilégiera l'utilisation de Smash : https://fromsmash.com/fr, qui est une plateforme de partage de fichier dont les serveurs sont basés en France. L'utilisation de plateformes dont les serveurs sont situés à l'étranger est proscrite (circulaire n° 6282-SG, obligation de mettre en place des solutions cloud souveraines hébergées en France).

Afin de compresser les PDF les plus volumineux, la collectivité met à votre disposition le logiciel **PDF24**.

11) Un usage privatif de la messagerie est toléré dans le cadre des nécessités de la vie courante et familiale. Dans ce cas, l'utilisateur fait apparaître dans le champ « Objet » du message le terme « PRIVE ». A défaut, le message est considéré comme professionnel.

Sous-chapitre 2 : Agenda électronique

12) L'usage privatif de l'agenda électronique est toléré dans les mêmes conditions que la messagerie électronique.

13) Les évènements personnels ne doivent pas apparaitre sur le calendrier professionnel, et peuvent être inscrit sur un calendrier personnel distinct.

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le
ID : 048-214801326-20250620-920062025-DE

14) Chaque service peut organiser des règles de partage étendues dans le cadre de son fonctionnement interne.

Chapitre 3 : Internet

15) Un accès à internet est mis à disposition des utilisateurs. Sont proscrits les usages suivants :

- la consultation ou téléchargement de données ayant un caractère illégal ;
- la consultation ou téléchargement de donnés ayant un caractère explicitement indécent, contraire à l'ordre public ;
- l'utilisation de son adresse professionnelle pour s'inscrire sur des sites ou des réseaux non liés à son activité professionnelle ;
- le téléchargement ou l'exploitation de tout ou partie des données numériques soumises au droit d'auteur sans autorisation et sans mention des crédits en cas de publication.
- le téléchargement de musique ou de vidéos sans lien avec l'exercice de ses fonctions ;
- l'expression sur des blogs, forum ou réseaux sociaux au nom de la collectivité sans habilitation ;
- l'utilisation professionnelle, sans autorisations de l'autorité territoriale, des plateformes d'échanges comme Facebook, Dropbox, Google Drive, One Drive… ;
- l'émission d'opinions personnelles étrangères à l'activité professionnelle susceptibles de porter préjudice à la collectivité ;
- la communication d'informations confidentielles ou protégées à des tiers sans autorisation ;
- accéder ou tenter d'accéder à un serveur ou à un poste de travail sans y avoir été préalablement habilité ;
- se livrer à des actions portant atteinte à la sécurité et au bon fonctionnement des serveurs, postes de travail et réseau de la collectivité ;
- déposer des données professionnelles sur des sites grand public ou sur des espaces personnels sans y avoir été autorisé ;
- utiliser le système d'information de la collectivité pour des activités rémunérées n'ayant aucun rapport avec l'exercice de ses fonctions.

16) Un usage privé d'internet est toléré dans le respect des règles énoncées ci-dessus et dans la mesure où il ne porte pas atteinte à l'exercice des fonctions de l'utilisateur. La collectivité ne saurait être tenue pour responsable de toute infraction commise par un utilisateur ne se conformant pas aux règles.

Chapitre 4 : Téléphones fixes

17) Les communications personnelles doivent être limitées aux cas d'urgence. Ces communications ne doivent pas perturber le fonctionnement des services.

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le
ID : 048-214801326-20250620-920062025-DE

Chapitre 5 : Les outils de la mobilité

18) Certains utilisateurs peuvent être équipés de supports mobiles : téléphone portable, tablette, ordinateur portable, clé USB...

Ces outils sont attribués personnellement à l'agent dans le cadre de ses missions et pour un usage exclusivement professionnel.

19) L'utilisateur doit tout mettre en œuvre pour :

- prévenir le vol de ses équipements en ne les laissant pas dans un endroit sans surveillance ;
- protéger les équipements et les manipuler avec le plus grand soin ;
- ne jamais divulguer à quiconque son code PIN ou son mot de passe de connexion.

14) En cas de perte ou de vol, l'utilisateur doit avertir l'autorité territoriale et le délégué à la protection des données afin qu'il soit procédé, si possible à un blocage ou un effacement à distance des données présentes sur le matériel ainsi qu'à une évaluation d'impact lié à la perte des données concernées.

Chapitre 6 : Matériels et logiciels

20) L'utilisateur n'est pas habilité à installer des logiciels et programmes sur le serveur commun. Il est responsable des logiciels et programmes qu'il installe lui-même sur son poste de travail ou sur ses outils de mobilité.

21) L'utilisation de support personnel de stockage n'est pas autorisé, sauf sur dérogation de l'autorité territoriale.

22) L'utilisation de certificats électroniques remis à l'utilisateur pour signer des documents électroniques a la même valeur probante qu'une signature manuelle. Un certificat représente personnellement son porteur. Un certificat électronique est matérialisé par une clé d'authentification sur un support avec connecteur USB auquel est associé un code PIN. L'ensemble est placé sous l'entière responsabilité de son porteur qui doit en faire un usage strictement professionnel et prendre toutes les mesures pour en garantir la sécurité.
En cas de perte ou de vol, l'utilisateur a l'obligation d'informer l'autorité territoriale et le délégué à la protection des données afin de procéder à une demande de radiation du certificat auprès de l'autorité de certification.

Chapitre 7 : utilisation de l'IA

23) L'utilisation de ces outils ne doit pas remplacer la prise de décision humaine ni négliger l'expertise humaine et le raisonnement associé.

24) Les utilisateurs doivent être conscients que les réponses générées par des outils IA peuvent être sujettes à des erreurs et doivent être évaluées avec soin. Les réponses générées doivent être vérifiées et validées avant d'être partagées en interne (collaborateurs) ou en externe (clients, usagers, partenaires, ...)

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le
ID : 048-214801326-20250620-920062025-DE

25) Les utilisateurs doivent respecter le règlement général sur la protection des données et ne partager aucune donnée personnelle dans leurs interactions avec un outil IA. Les utilisateurs doivent respecter les politiques de sécurité et de confidentialité des données de la collectivité lors de l'utilisation de ces outils.

Chapitre 8 : Protection des données personnelles

26) La constitution de fichiers informatiques comportant des données à caractère personnel est obligatoirement faite dans le respect de la réglementation en vigueur. Les données recueillies sur un sujet doivent être **adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.** Le délégué à la protection des données est l'interlocuteur privilégié des élus et des agents de la collectivité pour toutes les questions touchant aux données personnelles.

27) L'image d'une personne ainsi que les enregistrement vidéos et sonores qui se rapportent à elle ne peuvent être utilisés ou diffusés sans son consentement écrit.
Les photos, enregistrement vidéos ou sonores pris dans le cadre des activités de la collectivité ou dans ses locaux ne peuvent pas être utilisées à des fins personnelles et ne peuvent pas être diffusés à l'extérieur sans le consentement de l'autorité territoriale.

Chapitre 9 : Sécurité du système d'information

28) L'utilisateur doit utiliser des mots de passe robustes conforme aux recommandations de la CNIL : https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

- les mots de passe doivent être composés d'au minimum 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux
  ou
- les mots de passe doivent être composés d'au minimum 14 caractères comprenant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire
  ou
- une phrase de passe doit être utilisée et elle doit être composée d'au minimum 7 mots

29) La lutte contre les malwares et ransomwares est une priorité. L'utilisateur accordera une vigilance accrue à l'usage de la messagerie, des services internet et des supports de stockage. Ils favorisent, en effet, l'installation et/ou la propagation de programmes ou fichiers malveillants susceptibles d'altérer ou de capter les données stockées sur le poste de travail de l'utilisateur à son insu.
Si l'utilisateur constate des dysfonctionnements inhabituels sur son poste de travail, il devra alerter sans tarder l'autorité territoriale et le prestataire informatique.

30) Concernant la messagerie, chaque utilisateur de la boite mail se doit d'être prudent avec les mails qu'il reçoit :

- Toujours vérifier si l'adresse de l'expéditeur correspond à son identité.
  Un mail envoyé (soi-disant) depuis la Préfecture de la Lozère mais finissant par @123mail.su permet de douter de l'identité de l'expéditeur

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le
ID : 048-214801326-20250620-920062025-DE

- Vérifier l'orthographe du mail
  Les spams ont tendance à être remplis de fautes
- Ne jamais ouvrir de pièce-jointe d'un mail douteux.
  Les virus peuvent se cacher derrière de simples documents bureautiques. Ne pas hésiter à lancer une analyse antivirus sur les pièces-jointes
- Ne jamais cliquer sur les liens provenant d'un mail douteux.
  Toujours passer sa souris sur le lien afin d'en vérifier l'URL
- Ne jamais répondre à un mail demandant des données sensibles (RIB, code bancaire, etc.)

31) Concernant les supports de stockage type clé USB : une vigilance particulière doit être portée sur les supports inconnus ou à usage personnel. Ils peuvent être porteur de virus, pouvant compromettre tout le système d'information :

- Ne pas brancher les clé USB d'origine inconnue
- Si une clé doit être branchée, réaliser une analyse antivirus (clic droit sur la clé > rechercher d'éventuels virus)

32) Toute tentative d'introduction volontaire de virus de la part d'un utilisateur fera l'objet de sanctions.

33) L'utilisateur doit signaler sans délai au délégué à la protection des données, à l'autorité territoriale toute tentative malveillante ou violation constatée.

34) Chaque utilisateur doit verrouiller son poste ou fermer sa session dès lors qu'il s'absente de son bureau et se déconnecter de toutes les applications métiers dès qu'il en n'a plus l'utilité.

Chapitre 10 : Contrôles mis en œuvre

35) Les contrôles ont les finalités suivantes :

- la protection des agents de la collectivité dans le cas où la levée de doute est nécessaire concernant un usage illicite par un tiers des informations placées sous sa responsabilité ;
- la prévention et la répression de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;
- la protection des intérêts de la collectivité auxquels sont attachés un caractère de confidentialité ;
- la sécurité et le bon fonctionnement technique du système d'information ainsi que la protection physique des installations ;
- la maintenance curative, préventive ou évolutive.

36) Les contrôles anonymes et non individualisés : Ils visent des informations techniques comme le flux des sites internet, le volume du courrier...

37) Les contrôles individualisés : Ces contrôles identifient nominativement un utilisateur. Ils ne peuvent être mandatés que par l'autorité territoriale en cas de doute ou de constat sur le non-respect des règles en vigueur.

38) Conformément aux recommandations émises par la CNIL et à la jurisprudence en vigueur, l'autorité territoriale ne peut accéder qu'aux informations de nature professionnelle, sauf injonction de justice.

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le
ID : 048-214801326-20250620-920062025-DE

39) L'informaticien peut, si l'autorité judiciaire l'exige ou sur requête de l'autorité territoriale, après avis motivé, accéder au poste de travail de l'utilisateur en sa présence ou celle d'un représentant du personnel.

40) L'autorité territoriale est le seul destinataire des résultats des contrôles. Il prend les décisions qui s'imposent au regard de ces résultats, notamment pour répondre aux requêtes des autorités judiciaires ou pour engager des sanctions ou des actions judiciaires adaptées aux circonstances.

41) Les données rassemblées par l'autorité territoriale lors des contrôles sont conservées pendant 6 mois. Tout utilisateur peut s'adresser directement au délégué à la protection des données s'il souhaite avoir des informations concernant ses données personnelles.

42) Chaque utilisateur est responsable pénalement, selon les dispositions prévues au Code pénal, pour les infractions qu'il aurait commises aux moyens des outils informatiques ou des moyens de communication mis à sa disposition par la collectivité.

43) Chaque utilisateur est responsable civilement pour les dommages qu'il aurait causés à autrui au moyen des outils informatiques ou des moyens de communication mis à sa disposition.

44) L'usage abusif des moyens de communication ou des ressources informatiques mis à disposition par la collectivité peut donner lieu au dépôt d'une plainte en justice ou d'une requête en indemnisation de dommage.

Chapitre 11 : Suivi des traces

45) Toute ressource informatique active génère des suivis d'événement qui peuvent être journalisés dans des fichiers qualifiés de « fichiers de traces ». Ces fichiers sont essentiels à l'administration des systèmes et constituent des aides utiles au diagnostic et à la supervision des ressources informatiques. Ces fichiers consignent toute information comme celles relatives à la messagerie (expéditeur, destinataire, date…) mais aussi les heures de connexion aux applications.

46) Ce type de traces existe pour l'ensemble des services internes, internet et de télécommunication. L'administrateur système doit, par ailleurs, s'assurer de la traçabilité des opérations de maintenance qui peuvent être réalisées par des personnels techniques internes ou des partenaires externes.

Toutefois, dans le cadre d'une procédure engagée par les autorités judiciaires et après accord de l'autorité territoriale, ces fichiers peuvent être mis à disposition ou transmis à la justice.

47) La durée de conservation de ces données est de 1 an à partir du jour de leur enregistrement.

Chapitre 12 : Respect de la charte

48) Le non-respect des règles et mesures de sécurité figurant dans la présente charte expose l'utilisateur, selon la gravité des infractions et leurs répercussions :

- à un simple rappel aux bonnes pratiques ;
- à des mesures disciplinaires ;
- à des poursuites civiles ou pénales conformément aux dispositions légales en vigueur.

Envoyé en préfecture le 24/06/2025
Reçu en préfecture le 24/06/2025
Publié le
ID : 048-214801326-20250620-920062025-DE

RECEPISSE CHARTE INFORMATIQUE

Je soussigné :

Nom :

Prénom :

Service :

Fonction :

Utilisateur des moyens informatiques et réseaux de la COLLECTIVITE, déclare avoir pris connaissance de la présente charte et m'engage à la respecter.

Fait à..... Le

Signature

Les données sont collectées par « COLLECTIVITE » pour assurer la sécurité du système d'information. Pour en savoir plus sur vos droits, ou pour réaliser une réclamation, contacter la COLLECTIVITE ou son DPD « adresses »

Fait en deux exemplaires :

un pour l'intéressé (agent – élu)

un pour la collectivité