Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

MAIRIE DE FLOURENS

Charte Informatique

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

1. VALIDITE DU DOCUMENT

Identification		
Auteur(s)	**Objet**	**Destinataire(s)**
Erreur ! Source du renvoi introuvable.	Charte Informatique	L'ensemble du personnel tous statuts confondus, ainsi qu'au personnel temporaire et aux élus.

Validité du document				
Action	**Date**	**Nom**	**Fonction**	**Visa**
Rédaction	03/03/2025	Emmanuel JAIME	Conseiller Municipal	☒
Approbation		Marion RIVOIRE	Maire	☒
Diffusion		Ensemble du personnel, des élus, et utilisateurs des services informatiques de la mairie de FLOURENS		☐
				☐

Historique des modifications			
Date création	**Date application**	**Version**	**Evolution**
03/03/2025	03/03/2025	1.0	Création du document - Version initiale
11/06/2026	11/06/2026	1.1	Modifications de certains paragraphes suite à relecture Maire de Flourens

Documents de référence	
Document	**Détail**
N/A	N/A

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

2. TABLE DES MATIERES

1. Validité du document 2
2. Table des matières 3
3. Introduction 5
3.1. Contexte et enjeux 5
3.2. L'objectif 5
3.3. Champ d'application 5
4. Composition du SI (système d'information) 6
5. Les règles générales d'utilisation 7
5.1. Principe général de responsabilité et obligation de prudence 7
5.2. Obligation générale de confidentialité 8
5.3. Les droits et les devoirs des utilisateurs 8
5.3.1. Un accès aux ressources réglementé 8
5.3.2. Une utilisation professionnelle des ressources 8
5.4. Les droits et les devoirs de la collectivité 9
5.4.1. La déclaration obligatoire 9
5.4.2. L'information individuelle 9
5.4.3. La disponibilité et l'intégrité du système d'information 9
5.5. L'analyse et le contrôle 10
5.6. Les sanctions 10
6. Les postes informatiques 10
7. Mot de passe 11
8. La messagerie 11
9. Utilisation des réseaux et Wi-Fi pro 12
10. Les sites internets 14
11. Les réseaux sociaux 15
12. Téléphone 15
13. Smartphones 15
14. Télétravail 16
15. Intelligence artificielle 16
16. Droit à la déconnexion 17
17. Conformité RGPD 17
18. Comportement en cas d'incident 18
18.1. Vol ou perte d'une ressource 18
18.2. Infection ou intrusion sur le poste de travail 19
18.3. Dysfonctionnement de l'équipement 19
18.4. Respect du matériel 20

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

19. Les bases légales 20
19.1. La Législation 20
19.2. Le Droit disciplinaire 21
19.3. Le Code de la propriété intellectuelle 21
19.3.1. Partie législative 21
19.4. Le Code Pénal 21
19.4.1. Partie législative 21
20. Réceépissé charte informatique 23
21. Annexe 1 – Engagement de confidentialité 24
22. Annexe 2 - POLITIQUE DES MOTS DE PASSE 25
23. Annexe 3 – Dispositions légales applicables 25

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

3. INTRODUCTION

3.1. Contexte et enjeux

Les différents outils technologiques utilisés offrent au personnel de la collectivité 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 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, etc...).

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.

3.2. 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.

3.3. Champ d'application

La présente charte s'applique à l'ensemble des utilisateurs du système d'information (S.I) de la Ville de Flourens, et notamment :

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

- Les élus
- Les agents municipaux (titulaires ou contractuels, stagiaires)
- Les vacataires
- Les stagiaires, apprentis ou équivalents
- Les intérimaires
- Les employés de sociétés prestataires
- Les visiteurs occasionnels qui seraient amenés à utiliser les outils S.I de la Ville de Flourens

Il appartient à chaque utilisateur de ne pas permettre l'accès au S.I à des tiers non autorisés.

Cette charte 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).

4. COMPOSITION DU SI (SYSTEME D'INFORMATION)

Le S.I. est composé des ressources et équipements suivants :

- Postes de travail (ordinateur fixe ou portable)
- Téléphones (fixe ou portable)
- Tablettes et smartphones
- Supports de stockage (clé USB, disque dur externe...)
- Câbles divers (Ethernet, HDMI, VGA...)
- Réseau informatique (routeurs, switchs, connectique filaire et Wi-Fi)
- Imprimantes, scanners, multifonctions
- Serveurs d'administration et serveurs hébergeant les logiciels métiers et les fichiers
- Données numériques

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

- Logiciels informatiques (logiciels métier, logiciel de messagerie, logiciels applicatifs...)
- Vidéoprotection
- Contrôle d'accès et alarmes des bâtiments
- Procédures d'utilisation, d'installation...

Cette liste n'est pas exhaustive, car le S.I est en constante évolution, des éléments pouvant s'y ajouter ou être supprimés à tout moment.

5. LES REGLES GENERALES 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 leurs seraient interdits.

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 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 doit se porter garant de l'image de l'institution.

En tout état de cause, les utilisateurs ne peuvent en aucun cas utiliser le S.I. pour se livrer à des activités susceptibles de porter préjudice à la Ville de Flourens de quelque manière que ce soit.

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.

5.1. Principe général de responsabilité et obligation de prudence

L'utilisateur est responsable des ressources informatiques qui lui sont confiées dans le cadre de ses missions et doit concourir à leur protection, notamment en faisant preuve de prudence.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

L'utilisateur doit s'assurer d'utiliser les ressources informatiques mises à sa disposition de manière raisonnable, conformément à ses missions.

5.2. Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations et en particulier des données personnelles, traitées sur le S.I. Pour plus de précision, voir l'engagement de confidentialité en annexe 1.

Il s'engage à prendre toutes les précautions utiles pour éviter que ne soient divulguées de son fait, ou du fait de personnes dont il a la responsabilité, ces informations confidentielles (personnelles, bancaires ou administratives).

5.3. Les droits et les devoirs des utilisateurs

5.3.1. Un accès aux ressources réglementé

Toute personne (agents, élus, prestataires) travaillant dans la collectivité dispose d'un droit d'accès au système d'information.

Ce droit d'accès est :

- Strictement personnel.
- Incessible.

5.3.2. 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). Une déclaration à la CNIL est obligatoire pour toute création de fichiers contenant des informations nominatives.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

- 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.

5.4. Les droits et les devoirs de la collectivité

5.4.1. La déclaration obligatoire

La loi "Informatique et Libertés" impose une déclaration préalable auprès de la « Commission Nationale de l'informatique et des libertés » (CNIL) de tout traitement automatisé d'informations nominatives permettant l'identification directe ou indirecte d'une personne.

5.4.2. L'information individuelle

L'employeur 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...).

5.4.3. La disponibilité et l'intégrité du système d'information

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 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

5.5. L'analyse et le contrôle

Pour des nécessités de sécurité, de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle du responsable informatique et de l'autorité territoriale, être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi relative à l'informatique, aux fichiers et aux libertés.

5.6. Les sanctions

La Loi, les textes réglementaires (cf chapitre 18) 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 (cf chapitre 18).

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.

6. LES POSTES INFORMATIQUES

- Un ensemble "matériels - système d'exploitation - logiciels" est mis à disposition de chaque utilisateur :
    - Matériel : unité centrale, écran, clavier, souris...,
    - Système d'exploitation : Windows ...,
    - Logiciel : pack bureautique, logiciels de communication, logiciels de gestion, applications spécifiques.
- Le matériel informatique est fragile, il faut en prendre soin et redoubler d'attention pour les écrans plats.
- 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 son PC (Ex. : maintenir enfoncées les touches 'Ctrl+Alt+Suppr' et cliquer sur 'Verrouiller l'ordinateur').

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

- En cas d'absence prolongée, l'utilisateur doit quitter les applications et verrouiller son PC.
- A la fin de sa journée de travail, l'utilisateur doit quitter les applications, arrêter le système par arrêt logiciel, éteindre l'écran et l'imprimante connectée directement à son ordinateur.
- Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tiers et régulièrement modifiés (deux fois par an).
- La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde quotidienne des informations.
- 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 dans le but de préserver la capacité de mémoire.
- Les supports amovibles (CD, clé USB, etc.) provenant de l'extérieur doivent être soumis à un contrôle antivirus préalable.

7. MOT DE PASSE

L'accès au S.I ou aux ressources informatiques mises à disposition est protégé par un mot de passe individuel. Le login (identifiant personnel) et le mot de passe doivent être saisis lors de chaque accès au S.I.

Ce mot de passe doit être gardé confidentiel par l'utilisateur afin de permettre le contrôle de l'activité de chacun. Le mot de passe doit être mémorisé et ne doit pas être écrit sur un fichier informatique ni sur un support facilement accessible par un tiers.

Il ne doit pas être transmis ou confié à un tiers ou être rendu accessible, même sur demande de la hiérarchie.

Pour plus de précision sur la composition du mot de passe, voir la politique des mots de passe pour les accès au S.I en annexe 2.

8. LA MESSAGERIE

- L'utilisation de la messagerie est réservée à des fins professionnelles.
- L'utilisateur veillera à ne pas ouvrir les courriels dont le sujet ou l'émetteur paraîtrait suspect.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

- Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'Autorité Territoriale ou le référent informatique (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 son supérieur hiérarchique.
- 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 signera tout courriel professionnel.
- L'utilisateur doit vérifier la liste des destinataires et respecter les circuits de l'organisation ou la voie hiérarchique le cas échéant.
- L'utilisateur doit vérifier le contenu et l'historique des messages transférés (gestion du "Répondre à tous").
- En cas d'absence prévisible, l'utilisateur devra mettre 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.
-

9. UTILISATION DES RESEAUX ET WI-FI PRO

Le réseau Wi-Fi (pro) de la Ville de Flourens obéit aux mêmes règles de sécurité que tout le reste du réseau filaire auxquels sont connectés les ordinateurs professionnels. Certains comportements considérés comme dangereux pour le S.I. de la Ville de Flourens, pourront entraîner la fermeture immédiate du compte utilisateur à titre préventif, afin de protéger le réseau d'une attaque potentielle.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

Les principaux comportements dangereux sont les suivants :

- Interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés,
- Accéder à des informations privées des autres utilisateurs sur le réseau,
- Détruire volontairement des informations sur un des systèmes connectés,
- Mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont l'utilisateur à l'usage,
- Utiliser, même avec leur accord, ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués, ou masquer son identité,
- Modifier la configuration réseau de son poste de travail informatique.

Chaque utilisateur est juridiquement responsable de l'usage qu'il fait de ses connexions. Il s'engage à respecter les règles de déontologie informatique et notamment :

- Ne pas diffuser ses identifiants de connexion (login et/ou mot de passe),
- Utiliser les moyens mis à sa disposition conformément aux lois et réglementations en vigueur, en particulier :
    - Sans porter atteinte à la vie privée de toute personne ou au secret des correspondances,
    - Sans intercepter tout message et communication émis par les réseaux,
    - Sans porter atteinte aux droits d'autrui ou à la sécurité des personnes,
- Ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :
    - D'altérer, de modifier des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau,
    - D'interrompre ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau,
    - De modifier ou de détruire des informations sur un des systèmes,
    - De se connecter ou d'essayer de se connecter sur un site sans y être autorisé,

L'ensemble des services utilisés génère, à chaque usage, «des fichiers de traces», historique des actions effectuées par les utilisateurs. Ces fichiers conservent des

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

informations : heure de connexion, identifiants de la connexion (adresse IP, adresse MAC de l'ordinateur depuis lequel les services sont utilisés).

Ces fichiers servent notamment à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés.

10. LES SITES INTERNETS

- 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 (pédopornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée).
- 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 permanent sur les postes de données téléchargées sur Internet est interdit.
- Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.
- 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.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

11. LES RESEAUX SOCIAUX

- L'utilisation des réseaux sociaux est réservée à des fins professionnelles.
- 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 sous l'Autorité territoriale.
- La distinction entre l'utilisation professionnelle et l'utilisation personnelle est exigée (création de deux profils)
- Les conditions d'utilisation et d'accès sont définies (restrictions et limites pratiques).

12. TELEPHONE

- L'utilisation des téléphones fixes et portables (si existants) 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 et sms).
- L'Autorité territoriale peut procéder au contrôle de l'ensemble des appels émis sur les matériels fournis.
- 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 si existant.
- L'utilisateur doit veiller à soigner sa présentation lors d'un appel pour faciliter son identification et/ou son service.

13. SMARTPHONES

- Le smartphone est un outil de travail dont l'usage personnel peut être autorisé (mention "personnel" pour messages personnels).

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

- Il n'est pas obligatoire de répondre aux appels ou aux mails en dehors du temps de travail (soir, week-end et congés).
- Le smartphone ne doit pas venir perturber une réunion ou un entretien qui sont des évènements sociaux qui nécessitent la présence physique et intellectuelle de chacun.

14. TELETRAVAIL

Le télétravail désigne une forme d'organisation du travail dans laquelle un travail, qui aurait pu être exécuté dans les locaux de l'administration, est effectué par un agent hors de ces locaux, de façon régulière et volontaire en utilisant les technologies de l'information et de la communication.

Le télétravailleur bénéficie des mêmes droits et est soumis aux mêmes obligations que les agents travaillant sur site, tels que décrits dans la présente charte.

15. INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle (IA) est un processus visant à simuler certains traitements de l'intelligence humaine : elle repose sur la création et l'application d'algorithmes exécutés dans un environnement informatique dynamique. Son but est de permettre à des ordinateurs d'imiter des raisonnements en se basant sur de l'apprentissage et en exploitant une grande quantité de données.

Les systèmes utilisant de l'intelligence artificielle sont encore sujets à des défaillances, à des attaques, ou peuvent avoir des impacts sur les individus ou sur la société.

Les agents de la collectivité sont autorisés à utiliser les outils de l'IA mis à disposition ou développé par la collectivité. Cependant, les données résultant de l'utilisation d'une IA peuvent être erronées et/ou incomplètes. Ces outils sont à utiliser avec discernement et ne dispensent pas les agents d'effectuer un contrôle a posteriori de leurs travaux et de leurs recherches afin d'en assurer leur fiabilité.

Les agents sont autorisés à utiliser les outils d'IA tiers (grand public ou non maitrisés par la collectivité) mais s'engagent à n'y saisir aucune donnée professionnelle confidentielle

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

et aucune donnée à caractère personnel concernant les agents de la collectivité ou bien les usagers des services publics.

16. DROIT A LA DECONNEXION

Le droit à la déconnexion s'entend comme le droit pour tout agent public de ne pas être connecté à un outil numérique professionnel en dehors de son temps de travail.

Ce droit, qui s'inscrit dans une démarche d'amélioration des conditions de travail et d'une meilleure conciliation entre la vie professionnelle et la vie personnelle, a pour objectif le respect des temps de repos et de congé.

Ainsi, ce droit permet aux agents publics de ne pas répondre aux sollicitations professionnelles en dehors des horaires de travail sans risque d'être sanctionnés.

Les règles suivantes peuvent être adoptées :

- Respecter un temps de déconnexion aux outils numériques professionnels d'au moins 11 heures entre 2 journées de travail.
- Respecter les périodes de repos, congés et disponibilité de l'ensemble des agents, périodes pendant lesquelles ils ne sont pas tenus de consulter leurs messages et de répondre aux sollicitations (à l'exception des agents en astreinte).
- En tout état de cause, l'Autorité territoriale doit s'abstenir de contacter leurs agents en dehors de leurs horaires de travail habituels, ainsi que pendant leurs congés ou en cas d'arrêt maladie, sauf nécessité de service ou urgence caractérisée (à définir avec les agents).
- Dans tous les cas, l'usage de la messagerie électronique, du téléphone professionnel ou de tout autre outil numérique en dehors des horaires de travail doit être justifié par la gravité, l'urgence et/ou l'importance du sujet en cause.

17. CONFORMITE RGPD

La Ville de Flourens se conforme à la réglementation européenne RGPD (Règlement général sur la protection des données 2016/679). Par conséquent, les données numériques à caractère personnel sont recueillies pour des finalités prédéterminées,

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

partagées avec des services identifiés et stockées pendant une durée de conservation précisée et acceptée par l'usager lors du recueil de consentement.

Les responsables de traitement précisent sur quelle base légale repose le traitement mis en place. Le consentement de la personne concernée n'est pas obligatoire dans les cas suivants :

- L'exécution d'un contrat ou de mesures précontractuelles,
- Une obligation légale (recensement de la population par l'INSEE, registre du personnel) l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique (fichier de l'administration fiscale...),
- La sauvegarde de l'intérêt vital d'une personne,
- L'intérêt légitime (prévention de la fraude, sécurité des réseaux...).

En dehors de ces cas, le recueil préalable et explicite du consentement de la personne concernée est obligatoire.

Les personnes concernées par les données à caractère personnel bénéficient d'un droit à l'information relatif à la collecte des données, d'un droit d'accès et de rectification de leurs données, d'un droit de retrait de consentement et d'une possibilité de s'opposer au traitement pour motif légitime.

Lorsqu'elles considèrent que leurs droits ont été bafoués, elles peuvent demander à la Ville de Flourens de les faire respecter et ont la possibilité d'introduire une réclamation auprès d'une autorité de contrôle telle que la CNIL (Commission Nationale de l'Informatique et des Libertés).

18. COMPORTEMENT EN CAS D'INCIDENT

18.1. Vol ou perte d'une ressource

En cas de vol ou perte d'équipement informatique (ordinateur, téléphone, smartphone) fourni par la Ville de Flourens, l'utilisateur doit informer au plus vite l'Autorité territoriale puis lui communiquer :

- Les circonstances de la perte ou du vol, pour permettre à la Ville de Flourens de décider de porter plainte.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

Attention : l'utilisateur ne doit pas porter plainte en son nom ; seule une personne habilitée peut porter plainte au nom de la Ville de Flourens,

- L'inventaire des données qui étaient présentes sur le matériel avec leur niveau de sensibilité et leur niveau de protection au moment de la perte ou du vol.

Dans le cas où la Ville de Flourens porte plainte, il lui faudra communiquer les adresses MAC du matériel aux autorités compétentes. Il faudra donc demander ces informations en amont au S.I.

18.2. Infection ou intrusion sur le poste de travail

En cas de suspicion ou de constatation d'événements pouvant porter atteinte à la sécurité du S.I. de la Ville de Flourens (par exemple, une intrusion ou une infection par un code malveillant sur le poste de travail ou sur des ressources informatiques), l'utilisateur ne doit pas tenter de résoudre lui-même l'incident.

Il doit prévenir l'Autorité territoriale qui prendra les dispositions nécessaires pour confiner et traiter l'incident.

L'utilisateur peut toutefois isoler l'ordinateur du réseau de la Ville en débranchant le câble réseau et en déconnectant le Wifi.

18.3. Dysfonctionnement de l'équipement

En cas de dysfonctionnement du matériel ou de non-respect des exigences précitées, une reconfiguration du système pourra être décidée.

Le cas échéant :

- L'Autorité territoriale réinitialisera l'équipement avec sa configuration initiale standard,
- L'Autorité territoriale ne restaurera pas les données professionnelles stockées sur le matériel ou les données marquées « usage personnel » ; la Ville de Flourens ne pourra être tenue pour responsable de la perte ou de l'altération des données ainsi que des conséquences qui s'ensuivront.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

18.4. Respect du matériel

Lors de sa prise de fonction, la mairie fournit du matériel à l'agent, pour l'exercice de ses fonctions. Il est de sa responsabilité de prendre soin du matériel qui lui a été confié.

De ce fait en cas de négligence flagrante ou de destruction volontaire du matériel, des sanctions pourront être prises par l'Autorité territoriale à l'encontre de l'agent.

19. LES BASES LEGALES

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.

19.1. La Législation

- Loi n° 78-17 du 6 janvier 1978 sur l'informatique, les fichiers, les libertés.

  Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.
- Loi n° 78-753 du 17 juillet 1978 et l'ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration.
- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Elle est destinée à favoriser le développement des nouvelles technologies notamment par les collectivités.
- Le règlement européen de protection des données personnelles (RGPD) du 27 avril 2016.
  Il a pour objet la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

19.2. Le Droit disciplinaire

- Code général de la fonction publique.
- Décret n° 89-677 du 18 septembre 1989 modifié relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux.
- Décret n° 92-1194 du 4 novembre 1992 modifié fixant les dispositions communes applicables aux fonctionnaires stagiaires de la fonction publique territoriale.
- Décret n° 88-145 du 15 février 1988 modifié pris pour l'application de l'article 138 de la loi du 28 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale et relatif aux agents non titulaires de la fonction publique territoriale.
- Décret n° 91-298 du 20 mars 1991 modifié portant dispositions statutaires applicables aux fonctionnaires territoriaux nommés dans des emplois permanents à temps non complet

19.3. Le Code de la propriété intellectuelle

19.3.1. Partie législative

Livre Premier : Le droit d'auteur, notamment ses articles L. 112-2 et s. disposent que l'on compte les logiciels parmi les œuvres encadrées par la protection accordée par le droit d'auteur.

Est également interdit, à l'utilisateur d'un logiciel, toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.

19.4. Le Code Pénal

19.4.1. Partie législative

Livre III / Titre 2 / Chapitre III : Des atteintes aux systèmes de traitement automatisé de données, notamment ses articles 323-1 et s. disposent que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, d'entraver ou fausser, d'introduire frauduleusement des données ... sont punis de peines d'emprisonnement et d'amendes. Ces peines sont renforcées s'agissant de système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

En application de l'article 323-5, peuvent être prononcées des peines complémentaires.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

20. RECEEPISSE CHARTE INFORMATIQUE

Je soussigné :

Nom :

Prénom :

Service :

Fonction :

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

Fait à :

Le :

Signature

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

21. ANNEXE 1 – ENGAGEMENT DE CONFIDENTIALITE

Engagement de confidentialité pour les utilisateurs ayant vocation à manipuler des données à caractère personnel.

L'utilisateur s'engage, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin de protéger la confidentialité des informations auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

L'utilisateur s'engage en particulier à :

- Ne pas utiliser les données auxquelles il peut accéder à des fins autres que celles prévues par ses attributions,
- Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales,
- Ne faire aucune copie de ces données, sauf si ces copies sont nécessaires à l'exécution de ses fonctions,
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données,
- Prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données,
- S'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données,
- En cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de ses fonctions, demeurera effectif, sans limitation de durée après la cessation de ses fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

L'utilisateur a été informé que toute violation du présent engagement l'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

22. ANNEXE 2 - POLITIQUE DES MOTS DE PASSE

La politique de mots de passe de la Ville de Flourens est définie comme suit :

- La longueur minimale du mot de passe doit être de 8 caractères,
- Le mot de passe doit contenir ces 4 types de caractères :
  - Une ou des lettres majuscules,
  - Une ou des lettres minuscules,
  - Un ou plusieurs chiffres,
  - Un ou plusieurs caractères spéciaux parmi les suivants : (~! @ # $% ^& * _-+ =' | \ \ (){}\ []:; «' <>,.? /).
  - Le mot de passe doit être changé tous les 6 mois.

23. ANNEXE 3 – DISPOSITIONS LEGALES APPLICABLES

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 principaux textes législatifs et réglementaires dans le domaine de la sécurité du S.I.

Textes législatifs
Code des relations entre le public et l'administration
Code de la propriété intellectuelle
Code de la sécurité intérieure
Code pénal
Code civil

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

Envoyé en préfecture le 16/10/2026
Reçu en préfecture le 16/10/2026
Publié le
ID : 031-213101843-20261015-CM202610_202698-DE

Loi n°84-53 du 26 janvier 1984 (art. 89 et 90) et le décret n° 89-677 du 18 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux.

Loi n°94-361 du 10 mai 1994 portant mise en oeuvre de la directive (C. E. E.) n° 91-250 du Conseil des communautés européennes en date du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur et modifiant le code de la propriété intellectuelle.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). Elle est destinée à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux.

Textes réglementaires

Décret n°92-1194 du 4 novembre 1992 (art. 6) fixant les dispositions communes applicables aux fonctionnaires stagiaires de la Fonction Publique Territoriale.

Décret n°88-45 du 15 février 1988 (art. 36 et 37) pris pour l'application de l'article 136 de la loi du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la Fonction Publique Territoriale et relatif aux agents contractuels de la Fonction Publique Territoriale.

Décret n°91-298 du 20 mars 1991 (art. 15) portant dispositions statutaires applicables aux fonctionnaires territoriaux nommés dans des emplois permanents à temps non complet.

Réglementation européenne

La convention européenne du 28/01/1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel.

- Elle définit les principes de base de la protection des données que les États doivent concrétiser dans leur ordre juridique interne. Elle exclut en principe les entraves aux flux transfrontières de données entre les parties.
- Elle règle la coopération entre États pour la mise en œuvre de la Convention, en particulier l'assistance qu'un État partie doit prêter aux personnes concernées ayant leur résidence à l'étranger. Enfin, elle met en place un Comité consultatif chargé en particulier de faciliter et d'améliorer son application.
-

Le règlement (UE) 2016/679 du 27 avril 2016 dit règlement général sur la protection des données (RGPD), 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.