065_2026_INF

Département des Yvelines
JOUARS-PONTCHARTRAIN

L'an deux mille vingt-six, le 4 juin à 19h30, le Conseil Municipal légalement convoqué, s'est réuni dans la salle du Conseil municipal en séance publique sous la présidence de **Monsieur Thomas MENGELLE-TOUYA.**

Date de la convocation : 29 mai 2026

EN EXERCICE : 29
PRESENTS : 23 ; 24 aux questions diverses
VOTANTS : 29

ETAIENT PRESENTS : Mesdames et Messieurs MENGELLE-TOUYA – STOOS – MAGNIER – RAMALHO-CLAUDIO (au point sur les questions diverses) – GAMPACKAT – GUEZENEC– GODIN – ROQUELLE – COSTARD – SUTRA – BOGE – GISQUET – LOTODE – DA COSTA – DEFRANCE – FAUCHERY – SEBASTIEN – WINTZENRIETH – DE SAINT POL – METAYER – THOMASSET – DILASSEUR – GOUSSEAU –LYNCH

ABSENTS EXCUSES :
Madame RAMALHO-CLAUDIO avait donné pouvoir à Monsieur GODIN
Monsieur BOYE avait donné pouvoir à Madame STOOS
Madame D'ASTA avait donné pouvoir à Monsieur MAGNIER
Madame HOURTOLOU avait donné pouvoir à Monsieur MENGELLE-TOUYA
Madame DUBUS avait donné pouvoir à Madame GUEZENEC
Monsieur LE PAVEC avait donné pouvoir à Monsieur GAMPACKAT

SECRETAIRE DE SEANCE : Madame GUEZENEC

INFORMATIQUE
Charte informatique

Les élus, le conseiller spécial du Maire, ainsi que les agents communaux sont amenés à utiliser le matériel informatique communal.
Il y a lieu d'encadrer cette utilisation par l'adoption d'une charte informatique.

Vu le code général des collectivités territoriales ;
Vu l'avis favorable du comité social territorial en date du 22 mai 2026 ;

Considérant la nécessité d'adopter une charte informatique ;

Le Conseil municipal, après avoir délibéré, à l'unanimité,

➔ **ADOPTE** la charte informatique tel qu'annexée à la présente délibération

Fait et délibéré en séance, les Jour, Mois et An susdit
Ont signé au registre, le Maire et le secrétaire de séance.

Le secrétaire de séance

Morgane GUEZENEC

Le Maire

Thomas MENGELLE-TOUYA

Acte exécutoire

Mis en ligne le : 10 JUIN 2026

Cette délibération peut faire l'objet d'un recours contentieux devant le tribunal administratif dans un délai de deux mois à compter de l'accomplissement des mesures de publicité et de transmission en Préfecture. Elle peut également faire l'objet d'un recours gracieux adressé à Monsieur le Maire. Cette démarche proroge le délai de recours contentieux qui doit alors être introduit dans les deux mois suivant la réponse.

CHARTE INFORMATIQUE

Usage des systèmes d'information de la Commune

Document	Charte informatique et d'utilisation des systemes d'information
Version	1.0
Date d'approbation	(A compléter à la date de décision)
Applicable à	Elus, personnel communal, police municipale, prestataires
Autorité	Maire - Direction générale des services – conseiller délégué à la sécurité numérique

Ce document est soumis à approbation du Conseil Municipal.

Préambule

La commune de JOUARS PONTCHARTRAIN, collectivité territoriale de 6 000 habitants, met à disposition de ses agents, élus et prestataires des outils informatiques et numériques dans le cadre de l'exercice de leurs missions de service public.

La présente charte a pour objet de définir les règles d'utilisation des systèmes d'information (SI) de la commune, d'assurer la sécurité des données publiques et personnelles, et de préciser les droits et responsabilités de chaque utilisateur.

Elle s'inscrit dans le respect du Règlement General sur la Protection des Données (RGPD), de la loi Informatique et Libertés, ainsi que des dispositions du Code général de la fonction publique.

Article 1 - Champ d'application

1.1 Personnes concernées

La présente charte s'applique à l'ensemble des utilisateurs des systèmes d'information communaux :

- Les 29 élus du Conseil Municipal, incluant le Maire, les adjoints et les conseillers municipaux
- Le conseiller spécial du Maire
- L'ensemble du personnel communal, titulaires et contractuels, de tous les services
- Les stagiaires, apprentis et agents mis à disposition
- Les prestataires et fournisseurs disposant d'un accès au SI communal

Chaque utilisateur est tenu de prendre connaissance de la présente charte avant toute utilisation des ressources informatiques.

1.2 Ressources concernées

La charte couvre l'ensemble des ressources informatiques mises à disposition :

- Postes de travail fixes et portables
- Téléphones mobiles professionnels et tablettes
- Equipements de la Police Municipale (radios, terminaux, cameras piétons)
- Equipements de communication et de transmission spécifiques (radios du CTM, centre de loisir…)
- Accès Internet et messagerie électronique professionnelle
- Applications métiers (état civil, finances, urbanisme, scolaire, police...)
- Réseaux locaux, Wi-Fi et connexions distantes (VPN)
- Systèmes de vidéoprotection et de surveillance
- Services cloud et plateformes numériques officielles

Article 2 - Mise à disposition des moyens informatiques

2.1 Attribution des ressources

Les ressources informatiques sont attribuées à chaque utilisateur par le Responsable des Systèmes d'Information (RSI) ou la direction du service concernée, selon les besoins propres à chaque poste et service. Toute demande de matériel ou d'accès supplémentaire doit être formalisée par écrit et validée par le responsable hiérarchique. Le dernier contrôle de validité est réalisé par le conseiller délégué à la sécurité numérique. Le responsable informatique/téléphonie est chargé du

déploiement, maintenance et mise en condition opérationnelle des matériels sus mentionnés. Il est également chargé du suivi et de la bonne restitution des dits matériels.

2.2 Usage professionnel

Les outils informatiques communaux sont destinés en priorité à un usage professionnel. Un usage personnel ponctuel et raisonnable est toléré à condition :

- De ne pas nuire aux performances du réseau ou des équipements
- De ne pas interférer avec l'activité professionnelle
- De respecter les dispositions légales en vigueur
- De ne pas engager la responsabilité de la commune

Cet usage personnel demeure sous la responsabilité pleine et entière de l'utilisateur.

2.3 Dispositions spécifiques aux élus

Les 29 élus municipaux ainsi que le conseiller spécial bénéficient d'un accès aux outils numériques communaux dans le cadre strictement délimité de leurs missions électives. L'accès aux données personnelles des administrés est limité aux seules informations nécessaires à l'exercice de leur mandat.

Dans le cadre de l’exercice de leur mandat, les élus peuvent être amenés à accéder à des informations et données à caractère personnel, y compris sensibles.

À ce titre, ils s’engagent à :

- Respecter strictement la confidentialité des informations auxquelles ils ont accès, conformément au Règlement général sur la protection des données et à la législation en vigueur ;
- N’utiliser ces données que pour les besoins strictement liés à l’exercice de leur mandat, dans le respect des finalités pour lesquelles elles ont été collectées ;
- Ne pas divulguer, transmettre ou rendre accessibles ces informations à des tiers non autorisés, y compris à d’autres élus ou agents n’ayant pas à en connaître ;
- Veiller à la sécurité des supports et outils utilisés (poste informatique, messagerie, documents papier, supports amovibles), afin de prévenir tout accès non autorisé, perte ou divulgation ;
- Éviter l’utilisation d’outils ou de services non sécurisés ou non validés par la collectivité pour le traitement de données personnelles.

Cette obligation de confidentialité s’applique pendant toute la durée du mandat et perdure après sa cessation.

Tout manquement à ces règles est susceptible d’engager la responsabilité de l’élu et d’exposer la collectivité à des sanctions, notamment de la part de la Commission nationale de l'informatique et des libertés.

2.4 Dispositions spécifiques à la Police Municipale

Les agents de la Police Municipale bénéficient d'équipements et d'applications dédiées à leurs missions. L'utilisation de ces outils est régie par les dispositions légales spécifiques à la police municipale, notamment :

- Les règles d'accès aux fichiers de police et de sécurité publique
- La gestion des cameras piétons (le cas échéant) et des enregistrements (conservation, accès, destruction)
- L'utilisation des radios et terminaux de communication sécurises

- La traçabilité obligatoire des accès aux fichiers sensibles

Article 3 - Règles de sécurité informatique

3.1 Identifiants et mots de passe

Chaque utilisateur dispose d'un identifiant nominatif et d'un mot de passe personnel et confidentiel. Il lui est formellement interdit de :

- Communiquer ses identifiants à un tiers, quel qu'il soit
- Utiliser les identifiants d'un autre utilisateur
- Laisser sa session ouverte sans surveillance

Les mots de passe doivent respecter les exigences suivantes :

- Longueur minimale de 12 caractères
- Combinaison de majuscules, minuscules, chiffres et caractères spéciaux
- Renouvellement tous les 90 jours maximum
- Interdiction de réutiliser les 5 derniers mots de passe

3.2 Protection des équipements

Tout utilisateur est responsable du matériel qui lui est confié. Il doit :

- Ne jamais laisser un équipement portable sans surveillance dans un lieu public
- Signaler immédiatement toute perte, vol ou anomalie au RSI
- Verrouiller systématiquement sa session en cas d'absence du poste
- Ne pas connecter de supports externes (clés USB, disques) non autorisés

3.3 Mises à jour et antivirus

Les mises à jour de sécurité sont déployées par le service informatique. Les utilisateurs ne doivent pas bloquer, différer ou contourner ces mises à jour. Toute détection d'un comportement anormal du système doit être signalée sans délai.

3.4 Incidents de sécurité

Tout incident de sécurité (tentative de phishing, logiciel malveillant, accès non autorisé, perte de données) doit être signale immédiatement au RSI, au maire ou son conseiller délégué et, le cas échéant, au Délégué à la Protection des Données (DPO). Une procédure de gestion des incidents est disponible auprès du service informatique.

Article 4 - Protection des données personnelles (RGPD)

4.1 Principes fondamentaux

La commune est responsable de traitement au sens du RGPD. Chaque utilisateur qui accède ou traite des données à caractère personnel doit respecter les principes suivants :

- Licéité, loyauté et transparence dans le traitement
- Limitation des finalités : les données ne sont utilisées qu'aux fins pour lesquelles elles ont été collectées
- Minimisation : seules les données nécessaires sont traitées
- Exactitude et mise à jour des données
- Limitation de la conservation selon les durées légales

- Intégrité et confidentialité : accès restreint aux personnes habilitées

4.2 Droits des personnes

Les agents sont tenus de répondre, en lien avec le DPO, aux demandes d'exercice de droits des administres (droit d'accès, de rectification, d'effacement, de portabilité, d'opposition). Ils se rapproche de leur hiérarchie et du conseiller délégué à la sécurité pour les assister dans cette démarche.

4.3 Transferts et partages de données

Toute transmission de données personnelles vers un tiers doit être encadrée par une convention ou un accord de traitement conforme au RGPD, préalablement validée par le DPO.

4.4 Données sensibles

Les données relevant de catégories particulières (sante, situation sociale, données judiciaires notamment pour la Police Municipale) font l'objet d'une protection renforcée. Leur accès est strictement limite aux agents ou élus dument habilités.

Article 5 - Messagerie électronique et Internet

5.1 Messagerie professionnelle

Chaque agent dispose d'une adresse électronique professionnelle au nom de la commune. L'usage de messageries personnelles (Gmail, Yahoo, etc.) pour des échanges professionnels est interdit. Les utilisateurs doivent :

- Vérifier l'identité des expéditeurs avant tout clic sur un lien ou pièce jointe
- Ne jamais transmettre d'informations sensibles par courriel non chiffré
- Signaler tout message suspect au service informatique (phishing, tentative d'escroquerie)
- Ne pas utiliser la messagerie professionnelle à des fins commerciales ou militantes

5.2 Usage d'Internet

L'accès à Internet est fourni à des fins professionnelles. Sont strictement interdits :

- La consultation de sites à caractère pornographique, violent, illégal ou discriminatoire
- Le téléchargement de logiciels non autorisés
- Les jeux en ligne, les paris et les achats personnels pendant le temps de travail
- L'utilisation de proxys ou outils de contournement de filtrage
- La diffusion de contenus portant atteinte à l'image de la commune
- La consultation et/ou le téléchargement de contenus multimédias n’étant pas en rapport avec la mission de l’agent.

5.3 Réseaux sociaux

L'utilisation des réseaux sociaux personnels pendant le temps de travail est limitée à des fins professionnelles. Les agents s'interdisent de publier des informations confidentielles sur la commune, ses agents ou ses administrés. Toute communication institutionnelle doit être validée par le service communication.

Article 6 - Vigilance et cybersécurité

6.1 Hameçonnage (phishing)

Face à la recrudescence des tentatives d'hameçonnage visant les collectivités, tout utilisateur doit redoubler de vigilance face aux courriels demandant des identifiants, des virements, ou contenant des pièces jointes inattendues.

6.2 Ingénierie sociale

Aucune information sensible (identifiants, données d'administres, informations financières) ne doit être communiquée par téléphone ou courriel sans vérification préalable de l'identité du demandeur via un canal indépendant.

6.3 Télétravail et/ou accès distants

Le travail à distance est autorisé uniquement via les solutions sécurisées mises en place par la commune. L'utilisation de réseaux Wi-Fi publics sans VPN pour accéder aux ressources communales est interdite.

Article 7 - Contrôles et traçabilité

7.1 Journaux d'activité

La commune est susceptible de journaliser les connexions au réseau, les accès aux applications, les échanges de messagerie et les navigations Internet à des fins de sécurité et de détection d'incident. Ces journaux sont conservés conformément aux durées légales.

7.2 Contrôles

Des contrôles techniques et organisationnels peuvent être effectués par le RSI ou la direction générale des services afin de vérifier le respect de la présente charte. Ces contrôles sont réalisés dans le respect des droits des agents et dans les limites fixées par la législation.

7.3 Droit à la vie privée

Les fichiers ou répertoires clairement identifiés comme personnels par l'utilisateur ne peuvent être ouverts par l'employeur qu'en présence de l'agent ou après l'avoir dument convoqué, sauf circonstance exceptionnelle (urgence, menace grave pour le SI).

Article 8 - Sanctions

Le non-respect de la présente charte est susceptible d'entrainer des sanctions proportionnées à la gravité des manquements constatés :

8.1 Sanctions disciplinaires

Tout manquement grave peut faire l'objet d'une procédure disciplinaire conformément au statut de la fonction publique territoriale, pouvant aller jusqu'à la révocation.

8.2 Sanctions pénales

Certaines infractions détachables du service peuvent également engager la responsabilité pénale de l'utilisateur, notamment au titre :

- De l'accès non autorisé à un système informatique (article 323-1 du Code pénal)
- De la violation du secret professionnel

- Des infractions à la loi Informatique et Libertés
- De la diffusion de contenus illicites

8.3 Mesures conservatoires

En cas de manquement avéré ou indices graves et concordants de manquements, la commune se réserve le droit de suspendre immédiatement l'accès aux systèmes d'information dans l'attente des investigations nécessaires.

Article 9 - Responsabilités

9.1 Responsable des Systèmes d'Information (RSI)

Le RSI est charge de la mise en œuvre technique de la sécurité informatique, de la maintenance des équipements, de la gestion des accès et de l'accompagnement des utilisateurs. Il est l'interlocuteur principal pour tout incident ou question relative à la sécurité du SI.

9.2 Délégué à la Protection des Données (DPO)

Le DPO, désigné par la commune conformément au RGPD, conseille et contrôle la conformité des traitements de données personnelles. Il est le point de contact pour les demandes des administres relatives à leurs droits.

9.3 Responsabilité des utilisateurs

Chaque utilisateur est responsable de l'usage qu'il fait des ressources informatiques mises à sa disposition. Il ne peut se retrancher derrière l'ignorance de la présente charte pour s'exonérer de sa responsabilité.

9.4 Responsabilité de l'encadrement

Les responsables de service, chefs de service et directeurs sont tenus de s'assurer que leurs collaborateurs ont pris connaissance de la charte et de signaler tout manquement constate.

Article 10 - Formation et sensibilisation

La commune s'engage à sensibiliser régulièrement ses agents aux risques informatiques et aux bonnes pratiques numériques :

- Formation à l'intégration de tout nouvel agent
- Sessions annuelles de sensibilisation à la cybersécurité
- Diffusion de messages de prévention en cas de menace identifiée
- Mise à disposition de guides pratiques par le RSI
- Exercices de simulation (faux phishing, test de mot de passe) à des fins pédagogiques

Article 11 - Révision de la charte

La présente charte est révisée de plein droit à l'occasion de changements majeurs du SI, de l'évolution de la règlementation ou d'un incident significatif. Toute mise à jour est portée à la connaissance de l'ensemble des utilisateurs et annexée au règlement intérieur.

Article 12 - Acceptation

La présente charte est remise à chaque utilisateur lors de sa prise de poste ou de sa prise de mandat. Elle est opposable des signatures du formulaire d'acceptation ci-joint. L'utilisation des ressources informatiques vaut acceptation tacite de ses dispositions.

Signatures

Pour la Commune,
Le conseiller délégué à la sécurité numérique

Signature :
Date : _____

L'utilisateur,
Nom, prénom, qualité :

Signature (Lu et approuve) :
Date : _____

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

En cas d'urgence cyber (attaque, ransomware, violation de données) :

- Couper le poste concerne du réseau (débrancher le câble réseau ou désactiver le Wi-Fi)
- Appeler immédiatement le RSI
- Ne pas éteindre le poste (préservation des traces)
- Ne pas payer de rançon sans avis du RSI et des autorités
- Signaler au CSIRT régional si nécessaire : urgencecyber.iledefrance.fr