

VOS CONTACTS SECURITÉ INFORMATIQUE ET PROTECTION DES DONNÉES

Sécurité Informatique

M. Samuel PIREZ – Responsable du Service Informatique – informatique@ville-vieux-conde.fr

Protection des données personnelles

M. Alexis GOURGUECHON – *Délégué à la Protection des Données* – agourguechon@valenciennes-metropole.fr

LA CHARTE D'UTILISATION DES MOYENS INFORMATIQUES ET DES OUTILS NUMERIQUES DE LA MAIRIE DE VIEUX-CONDE

TABLE DES MATIERES

ARTICLE 1.	OBJET DE LA CHARTE.....	3
ARTICLE 2.	SECURITÉ DU SYSTÈME D'INFORMATION	3
ARTICLE 3.	VIE PRIVÉE DE L'UTILISATEUR	3
ARTICLE 4.	CONFIDENTIALITÉ	3
ARTICLE 5.	MOYENS D'AUTHENTIFICATION.....	4
1.	Obligation de sécurisation des moyens d'authentification	4
2.	Interdiction de partage et de délégation des moyens d'authentification	4
3.	Le respect des règles relatives aux mots de passe (politique mots de passe).....	4
ARTICLE 6.	GESTION DU SYSTÈME D'INFORMATION	5
ARTICLE 7.	VIGILANCE DE L'UTILISATEUR ET OBLIGATION DE RAPPORT.....	5
ARTICLE 8.	INTÉGRITÉ DU SYSTÈME D'INFORMATION	5
1.	Intégrité du poste de travail	5
2.	Intégrité du réseau informatique de la Mairie	5
3.	Intégrité du système d'information.....	6
ARTICLE 9.	SÉCURITÉ DU POSTE DE TRAVAIL DE L'UTILISATEUR.....	6
ARTICLE 10.	MODALITÉS D'EXPRESSION DES UTILISATEURS	6
ARTICLE 11.	ACCÈS A INTERNET	6
ARTICLE 12.	MESSAGERIE ÉLECTRONIQUE	7
1.	Les courriers électroniques personnels.....	7
2.	L'utilisation de la messagerie électronique.....	7
3.	Bonnes pratiques	8
ARTICLE 13.	UTILISATION D'EQUIPEMENTS INFORMATIQUE MOBILES	8
ARTICLE 14.	UTILISATION DE TÉLÉPHONES FIXES	9
ARTICLE 15.	STOCKAGE DES DONNÉES	9
ARTICLE 16.	PROTECTION DES DONNÉES PERSONNELLES	10
ARTICLE 17.	PROPRIÉTÉ INTELLECTUELLE	10
ARTICLE 18.	SANCTIONS	10
ARTICLE 19.	AVIS DU COMITÉ TECHNIQUE ET ENTRÉE EN VIGUEUR.....	10
ARTICLE 20.	QUESTIONS	11

ARTICLE 1. OBJET DE LA CHARTE

La présente charte (Ci-après « Charte » ou La Charte ») a pour objet de contribuer à la présentation de la sécurité du système d'information de la Mairie de VIEUX-CONDE (Ci-après « La Mairie ») en faisant de l'Utilisateur quotidien, un acteur essentiel à la réalisation de cet objet et d'encadrer l'utilisation des moyens informatiques et des outils numériques par les agents (ci-après « Utilisateur »). Cette charte s'adresse donc à tous les agents qui sont tenus de s'y conformer ainsi qu'à toutes les personnes qui utilisent le réseau informatique de la commune.

Par cette charte, l'Utilisateur prend conscience des enjeux de sécurité informatique et de protection des données à caractère personnel.

L'Utilisateur est ainsi pleinement responsable de l'usage qu'il fait des ressources informatiques qui sont mises à sa disposition dans l'exercice de sa fonction. Il doit en réserver l'usage au cadre de son activité professionnelle.

ARTICLE 2. SECURITÉ DU SYSTÈME D'INFORMATION

L'Utilisateur s'engage à ne pas compromettre l'accès aux données et aux applications que ce soit de manière physique ou logicielle et de ne pas compromettre leur intégrité ou leur confidentialité.

L'Utilisateur s'engage notamment à ne contourner aucun des systèmes de sécurité mis en œuvre par la Mairie.

ARTICLE 3. VIE PRIVÉE DE L'UTILISATEUR

L'Utilisateur a la possibilité, à titre exceptionnel et pour un temps limité, d'utiliser les outils professionnels qui sont mis à sa disposition dans un cadre privé.

L'Utilisateur reste responsable de cette utilisation personnelle, et ne doit pas enfreindre les règles de la présente charte d'utilisation des moyens informatiques et des outils numériques.

ARTICLE 4. CONFIDENTIALITÉ

L'Utilisateur s'engage, conformément 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 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 pour l'exercice de sa mission ;
- Ne divulguer ces données à caractère personnel 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 à ce que cela soit nécessaire à l'exécution de la mission qui lui incombe ;
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de sa mission afin d'éviter l'utilisation détournée ou frauduleuse de ces données à caractère personnel ;
- S'assurer que seuls des moyens de communication sécurisés seront utilisés pour transférer les données à caractère personnel ;
- Restituer et détruire, l'intégralité des données à caractère personnel à la fin de la mission sauf obligations légales d'archivage.

L'Utilisateur doit être vigilant sur le risque de divulgation dans le cadre d'utilisation d'outils informatiques dans les lieux autres que ceux de La Mairie (transports en commun, lieux ouverts au public ...)

La violation de cet engagement de confidentialité expose l'Utilisateur à des sanctions disciplinaires et pénales conformément aux articles 226-16 à 226-24 du Code Pénal.

ARTICLE 5. MOYENS D'AUTHENTIFICATION

1. Obligation de sécurisation des moyens d'authentification

L'Utilisateur doit assurer la protection des moyens d'authentification (nom d'utilisateur, mots de passe, badge ...) qui lui ont été affectés sur tous les équipements mis à sa disposition par la Mairie, y compris les équipements mobiles.

L'Utilisateur doit prendre toutes les précautions nécessaires afin d'assurer la confidentialité des moyens d'authentification.

2. Interdiction de partage et de délégation des moyens d'authentification

L'Utilisateur ne doit pas se servir, d'un autre compte que celui qui lui a été attribué, pour accéder au système d'information de la Mairie.

L'Utilisateur s'engage à ne pas déléguer les droits d'utilisation du système d'information de la Mairie qui lui sont attribués, sauf lorsque les nécessités du service l'imposent et après accord écrit de sa hiérarchie.

3. Le respect des règles relatives aux mots de passe (politique mots de passe)

L'Utilisateur s'engage à respecter les règles mises en place pour le choix et la modification régulière des mots de passe. Les mots de passe de session répondent aux règles suivantes :

- Un dimensionnement d'au moins huit (8) caractères ;
- L'utilisateur doit changer le mot de passe tous les 64 jours.

L'Utilisateur s'engage à ne jamais communiquer son mot de passe.

ARTICLE 6. GESTION DU SYSTÈME D'INFORMATION

Les autorisations d'accès aux ressources informatiques, le choix et l'installation de matériels et de logiciels relèvent et sont effectués exclusivement par La Mairie.

ARTICLE 7. VIGILANCE DE L'UTILISATEUR ET OBLIGATION DE RAPPORT

L'Utilisateur s'engage à signaler, au Délégué à la Protection des Données (DPO), ou au Service Informatique ou à son supérieur hiérarchique, dans les plus brefs délais, toute tentative malveillante ou violation constatée, sur tous les supports, même papier, utilisé par l'Utilisateur.

Ces tentatives malveillantes ou violations constatées peuvent être :

- Tentative d'intrusion dans le système d'information de la Mairie (tentative de piratage) ;
- Email suspect (tentative d'hameçonnage, rançongiciel etc) ;
- Infection du système d'information par un virus ;
- Impossibilité d'accès à un logiciel ;
- Perte de données, perte de matériel nomade.

Cette liste des incidents n'est pas limitative

Cette remontée d'informations permettra aux services compétents d'adopter les mesures adaptées.

L'Utilisateur s'engage à informer le Délégué à la Protection des Données (DPO), ou le Service Informatique ou son supérieur hiérarchique, pour toute perte de matériel remis par la Mairie (badge, smartphone, clé USB etc).

L'Utilisateur veille à la sécurité des ressources informatiques mises à sa disposition. Ainsi, il doit verrouiller son ordinateur ou fermer sa session dès lors qu'il s'absente de son bureau, et se déconnecter de toutes les applications métiers dès qu'il n'en a plus l'utilité.

ARTICLE 8. INTÉGRITÉ DU SYSTÈME D'INFORMATION

1. Intégrité du poste de travail

Il est interdit de modifier la configuration matérielle et logicielle du poste de travail fourni par la Mairie.

Il est notamment interdit de connecter au poste de travail, tout dispositif mobile qui n'aurait pas été agréé par la Mairie (clé USB, Disque Dur externe, Graveur externe, carte mémoire ...)

Il est interdit de contourner les dispositifs de protection du poste de travail.

2. Intégrité du réseau informatique de la Mairie

Il est interdit de connecter, au réseau informatique de la Mairie, tout élément qui n'aurait pas été expressément autorisé par la Mairie, comme un ordinateur, un périphérique ou une borne d'accès de réseau sans fil.

3. Intégrité du système d'information

L'Utilisateur s'engage à ne pas introduire de données non répertoriées dans le Système d'Information de la Mairie.

L'Utilisateur ne tentera pas d'y accéder sans autorisation et ne supprimera aucun fichier ou données (de tiers ou fichiers systèmes) pouvant mettre en cause l'intégrité du Système d'information ou l'activité de la Mairie.

ARTICLE 9. SÉCURITÉ DU POSTE DE TRAVAIL DE L'UTILISATEUR

L'Utilisateur s'engage à ne pas télécharger ou charger des programmes malveillants. Il est responsable de l'utilisation des programmes de sécurité de son poste de travail, qui ne doivent en aucun cas être désactivés.

L'Utilisateur veille aussi à installer les mises à jour des différents logiciels et applicatifs métiers quand elles sont disponibles.

ARTICLE 10. MODALITÉS D'EXPRESSION DES UTILISATEURS

Il est interdit pour l'Utilisateur de transmettre ou publier des messages contribuant à du harcèlement moral ou sexuel, prenant la forme de menaces verbales ou physiques ou de transmettre ou relayer des messages de type canulars, chaînes de messages électroniques, rumeurs diverses etc.

ARTICLE 11. ACCÈS A INTERNET

La Mairie, met à disposition de l'Utilisateur, une connexion internet sécurisée.

Il est interdit à l'Utilisateur d'utiliser le réseau internet de la Mairie à des fins commerciales ou pour soutenir des activités lucratives.

La Mairie interdit aux Utilisateurs :

- La consultation ou le téléchargement de données ayant un caractère illégal (pédophilie, corruption de mineurs sur internet, incitation à la haine raciale ou provocation à la discrimination de personnes en raison de leurs origines ou de leur appartenance ou non à une ethnie ou une religion déterminée, de leur sexe, de leur orientation sexuelle ou de leur handicap, menace ou incitation à la violence, Trafic illicite, mise en danger de la vie d'autrui, incitation à commettre des infractions, spams, injure, diffamation, pornographie, pédopornographie, xénophobie, racisme, escroquerie, fait contraire à l'ordre public et aux bonnes mœurs, à la dignité de la personne humaine et à la vie privée des personnes ;
- Le téléchargement de musiques, vidéos ou tout autre contenu en ligne n'étant pas en lien direct avec l'exercice des missions de l'Utilisateur ;

- L'utilisation professionnelle, sauf autorisation expresse, d'applicatifs non autorisés par la Mairie (DROPBOX, WETRANSFER, GOOGLE DRIVE, GOOGLE FORMS, ONEDRIVE, ICLOUD)
- La communication d'informations confidentielles ou protégées par la législation en vigueur
- Diffuser et publier des données professionnelles et des données à caractère personnel sur des sites grand public ou sur des espaces personnels sans en avoir été habilités ;

L'Utilisateur ne peut mettre à jour ou créer, au moyen de l'infrastructure d'accès à internet fournie par la Mairie, tout site internet comme des pages personnelles, blog, réseau sociaux ou site internet collaboratif) sauf dans le cadre d'une mission de l'agent.

La mairie met en place un dispositif de filtrage des contenus internet afin d'assurer la sécurité de son système d'information, et recueille à ce titre, un certain nombre de données :

- Le poste informatique à l'origine de la consultation
- Le type de ressource consultée
- La durée de consultation
- La date et horaire de consultation

L'ensemble de ces données sont conservées pour une durée de 30 jours.

Il est interdit à l'Utilisateur d'accéder à des sites payants, de participer à des jeux en ligne, d'entretenir sur internet des relations commerciales à titre privé.

ARTICLE 12. MESSAGERIE ÉLECTRONIQUE

1. Les courriers électroniques personnels

La Mairie fournit à l'Utilisateur une adresse professionnelle de messagerie électronique pour les besoins de ses missions.

Les courriers électroniques reçus sur cette messagerie sont présumés professionnels et peuvent être consultés par la Mairie et les supérieurs hiérarchiques de l'Utilisateur.

Les messages personnels, identifiés comme tel notamment en le précisant dans leur objet ou stocké dans un répertoire intitulé « Personnel » ou « Privé » ne peuvent être consultés librement par l'employeur en vertu du principe fondamental du secret des correspondances privées.

La Mairie peut cependant consulter les messages personnels de l'Utilisateur en cas d'enquête judiciaire ou de décision judiciaire ordonnant à la Mairie de consulter les mails personnels de l'Utilisateur.

2. L'utilisation de la messagerie électronique

L'Utilisateur ne peut utiliser la messagerie électronique pour les agissements fautifs suivants :

- Echange d'information confidentielles sans protection adéquate et autorisée
- La redirection de la messagerie professionnelle vers une messagerie personnelle

- L'échange de messages à caractère xénophobe, raciste, diffamatoire, homophobe ou des contenus pornographique et pédopornographiques ou contraire à l'ordre public et aux bonnes mœurs
- L'échange de messages sous identifiant différent de celui de l'Utilisateur
- D'une manière générale, l'Utilisation de la messagerie électronique dans des conditions susceptibles de porter atteinte à l'image, à la réputation ou à la sécurité d'autrui ou de l'employeur au bon fonctionnement du Système d'Information de la Mairie.

Pour l'envoi de documents par voie électronique contenant des données à caractère personnel ou des informations confidentielles, l'Utilisateur doit éviter l'usage de la messagerie électronique, et préférer l'utilisation de plateforme sécurisée comme : www.framadrop.org

3. Bonnes pratiques

Le champ « destinataire » symbolisé par « À : » est réservé aux personnes devant mener une action relative au contenu du courriel.

Le champ « copie » symbolisé par « Cc : » est destiné aux personnes destinataires du courriel pour information.

Le champ « copie Carbonne invisible » symbolisé par « Cci : » est utilisé pour la protection de la vie privée des destinataires lorsqu'on ne désire pas divulguer leur adresse de messagerie. Hors cette hypothèse, l'utilisation de ce champ doit être limitée.

L'Utilisateur s'engage :

- À ne pas envoyer de copies (Cc ou Cci) a un nombre important de destinataires ;
- À rédiger des objets de mail clairs et précis pour chacun de ses courriels ;
- À être courtois dans tous ses échanges électroniques ;
- À ne pas créer ou transférer des messages publicitaires non sollicités (spams) depuis les ressources informatiques de la Mairie.

L'Utilisateur est informé que la fonction « Répondre à Tous » ne doit pas être utilisé systématiquement, notamment dans le but de ne pas encombrer les boîtes aux lettres des destinataires.

Si l'Utilisateur reçoit un courriel qui lui paraît suspect, il s'engage à ne pas l'ouvrir et à avertir le Service Informatique

ARTICLE 13. UTILISATION D'EQUIPEMENTS INFORMATIQUE MOBILES

La Mairie qualifie d'équipements informatique mobiles, tout support numérique permettant le travail à distance (tablette, ordinateur portable, smartphone, clé USB, disque dur externe).

L'Utilisateur s'engage à :

- Ne pas laisser les équipements mobiles dans un endroit sans surveillance ;
- Manipuler le matériel avec toutes les précautions utiles ;
- Ne jamais divulguer ses identifiants, son code PIN, son mot de passe ;

- Avertir le Directeur Général des Services ou le Responsable Informatique, ou le Délégué à la Protection des Données ou le Référent Informatique et Libertés en cas de perte ou de vol dès que cela survient, afin qu'il soit procédé à toutes mesures techniques et administratives liées à la perte des données concernées ;
- Eviter de connecter son matériel à un réseau Wi-Fi public ou inconnu et échanger aucune information confidentielle.

L'Utilisateur s'engage à mettre sur des périphériques de stockage nomades (ex : Clé USB) que les données strictement nécessaires à l'accomplissement de sa mission et s'assure que ces données sont sauvegardées sur le Réseau Informatique de la Mairie.

ARTICLE 14. UTILISATION DE TÉLÉPHONES FIXES

La Mairie met à disposition de ses agents, une ligne fixe pour les communications professionnelles.

L'Utilisateur est autorisé à utiliser, de manière limitée, cette ligne fixe pour un usage personnel.

ARTICLE 15. STOCKAGE DES DONNÉES

L'Utilisateur s'engage à respecter les consignes qui lui sont communiquées en matière de stockage et de sauvegarde des données. Il est tenu de garantir la disponibilité des données stockées sur son poste de travail.

L'Utilisateur ne doit pas mettre en place des mesures qui restreignent l'accès pour les autres Utilisateurs autres que celles prévues par la Mairie.

Il sera rappelé que constitue une faute, le fait, pour l'Utilisateur, de rendre inaccessible l'accès aux fichiers de son poste de travail (les fichiers personnels et les fichiers professionnels) notamment en recourant à des dispositifs de chiffrement.

L'Utilisateur veillera particulièrement à respecter les règles de confidentialité décrites à l'article 3 de la présente Charte et à ne pas disséminer, en dehors de l'entreprise, des documents auxquels il a eu accès dans le cadre professionnel, notamment par voie de stockage sur des supports acquis à titre personnel ou via des logiciels et applicatifs de transferts de fichiers (Ex : le Logiciel gratuit en ligne WETRANSFER ou le logiciel gratuit DROPBOX).

La Mairie concède à l'Utilisateur, la possibilité, pour un volume qui doit rester raisonnable, de stocker des fichiers personnels sur les moyens informatiques qui sont mis à sa disposition. Ces fichiers doivent être rangés dans un répertoire ou dossier nommé « PERSONNEL », et ne pas être contraire à la loi ou aux bonnes mœurs, et notamment la législation anti-piratage et à la propriété intellectuelle. Il est néanmoins rappelé à l'Utilisateur que la Mairie pourra lui demander l'accès à ce fichier, en sa présence, ou hors de sa présence en cas de risques ou d'événements particuliers (Ex : enquête judiciaire).

ARTICLE 16. PROTECTION DES DONNÉES PERSONNELLES

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable.

L'Utilisateur s'engage à consulter le Délégué à la Protection des Données ou le Référent Informatique et Libertés de la Mairie pour toute nouvelle utilisation de données personnelles (nouveau fichier, sondage / enquête de satisfaction, utilisation d'un nouveau logiciel etc).

La constitution de fichiers bureautiques intégrant des données personnelles ne doit pas être réalisée sans l'avis du Délégué à la Protection des Données. Cette démarche s'inscrivant dans la mise en œuvre du Règlement Général UE 2016/679 du 27 avril 2016 relative à la protection des données personnelles (RGPD) dans la Mairie.

ARTICLE 17. PROPRIÉTÉ INTELLECTUELLE

L'Utilisateur ne recourra en aucune manière, aux ressources informatiques de la Mairie, notamment les moyens de communication électronique, mises à sa disposition par la Mairie, pour lire, copier, stocker ou transmettre, sans licence et à des fins privées ou commerciales, des contenus ou des logiciels protégés par le droit d'auteur et plus largement les dispositions du Code de la Propriété Intellectuelle.

ARTICLE 18. SANCTIONS

L'Utilisateur est responsable pénalement des infractions prévues par les dispositions du code Pénal relatives aux atteintes aux systèmes de traitement automatisé de données (art. 323-1 et suivants du Code Pénal).

L'Utilisateur est aussi responsable civilement pour tous les dommages qu'il aurait causés par ou au moyen des outils informatiques ou des moyens de communication mis à sa disposition par la Mairie selon les articles 1240 et suivants du Code Civil (anciennement art. 1382 et suivants du Code Civil).

Le non-respect des règles et mesures de sécurité de la présente charte expose l'Utilisateur a des sanctions déterminées en fonction de la gravité de l'infraction et de ses répercussions à :

- Un rappel à la loi et aux bonnes pratiques ;
- Des mesures disciplinaires ;
- Des poursuites civiles et/ou pénales conformément aux lois en vigueur.

ARTICLE 19. AVIS DU COMITÉ TECHNIQUE ET ENTRÉE EN VIGUEUR

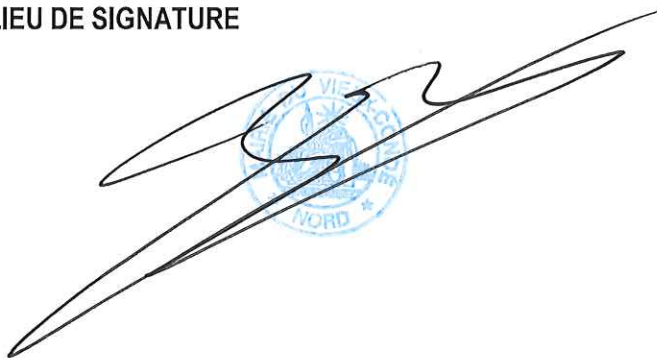
Le comité technique a émis un avis favorable de la présente charte le 02 Mars 2022

La présente charte entre en vigueur à compter du 15 Mars 2022

ARTICLE 20. QUESTIONS

Pour toute question relative au contenu de la présente, merci de vous adresser aux personnes figurant dans l'encart « VOS CONTACTS SECURITÉ INFORMATIQUE ET PROTECTION DES DONNÉES ».

DATE ET LIEU DE SIGNATURE

A handwritten signature in black ink is written over a blue circular stamp. The stamp contains the text "VIE" at the top and "MORD" at the bottom, with a central emblem. The signature is a stylized, cursive script.