



# CHARTRE INFORMATIQUE

Envoyé en préfecture le 17/04/2024

Reçu en préfecture le 17/04/2024

Publié le

ID : 083-218300903-20240408-D2024\_04\_4\_12-DE

**Les collaborateurs sont tenus à des obligations en matière d'utilisation des équipements et logiciels mis à leur disposition dans le cadre de leurs activités professionnelles.**

## LES OBLIGATIONS ET RESPONSABILITÉS EN MATIÈRE DE SÉCURITÉ INFORMATIQUE

### Protéger les données personnelles



Je mets en évidence les données considérées privées, en faisant figurer << PRIVE >> en tête du nom, des dossiers, et de l'objet des courriels.

Consulter la fiche «Comment protéger les données personnelles ?»

### Verrouiller mon ordinateur



Je verrouille mon poste de travail dès que je m'absente afin de protéger mon travail [touche  + L ou Ctrl + Alt + Suppr]

Consulter la fiche «Comment bien utiliser mon ordinateur ?»

### Ranger mon bureau



Au bureau, je ne laisse pas mes documents à la vue de tous car je risque d'exposer des informations confidentielles.

Consulter la fiche «Comment obtenir un bureau propre ?»

### Stocker mes fichiers sur les serveurs



Je stocke mes données de travail sur les serveurs car ce sont les seuls espaces de stockage sécurisés et sauvegardés.

Consulter la fiche «Comment stocker sur les serveurs ?»

### Utiliser uniquement les clés USB autorisées



Je ne connecte que des clés USB fournies par la DSI car je risque d'introduire un virus dans le système informatique.

Consulter la fiche «Comment obtenir une clé USB autorisée ?»

### Protéger mes mots de passe



Je garde secrets mes mots de passe parce que je suis responsable de toute action réalisée à partir de mon compte

Consulter la fiche «Comment protéger mon mot de passe ?»

### Protéger ma boîte mail



Je ne clique ni sur les liens ni sur les documents joints avant de m'être assuré qu'ils ne sont pas malveillants.

Consulter la fiche «Comment protéger ma boîte mail ?»

### Respecter les règles du télétravail



Je suis scrupuleusement les consignes de télétravail pour ne pas exposer d'avantage le système informatique à des attaques.

Consulter la fiche «Comment télétravailler en sécurité ?»

## SANCTIONS DISCIPLINAIRES



Groupe	Sanctions
1er Groupe	<ul style="list-style-type: none"><li>• Avertissement Blâme</li><li>• Exclusion temporaire de fonctions de 1 à 3 jours</li></ul>
2ème Groupe	<ul style="list-style-type: none"><li>• Radiation du tableau d'avancement</li><li>• Abaissement d'échelon immédiatement inférieur à celui détenu par le fonctionnaire.</li><li>• Exclusion temporaire de fonctions de 4 à 15 jours maximum.</li></ul>
3ème Groupe	<ul style="list-style-type: none"><li>• Rétrogradation au grade immédiatement inférieur, à l'échelon comportant un indice égal ou immédiatement inférieur à celui détenu par le fonctionnaire</li><li>• Exclusion temporaire de fonctions de 16 jours à 2 ans</li></ul>
4ème groupe	<ul style="list-style-type: none"><li>• Mise à la retraite d'office</li><li>• Révocation</li></ul>

## LES RESPONSABILITÉS CIVILES ET PÉNALES.

La négligence, l'imprudence ou la malveillance d'un utilisateur sont de nature à engager sa responsabilité pénale. Conformément à l'article 1240 et suivants du Code civil, la responsabilité civile de l'agent pourra également être engagée.



## IMPORTANT

Lorsque l'on quitte son bureau il est important de verrouiller sa session, pour plusieurs raisons de sécurité.

# VERROUILLER SON POSTE DE TRAVAIL

Ce qu'il peut se passer lorsque vous ne verrouillez pas votre poste de travail :

01

N'importe quelle personne ayant accès physiquement à votre poste pourrait **avoir accès facilement aux fichiers qui s'y trouvent, et les récupérer** (documents ouverts en cours, parfois confidentiels ou tout simplement privés)

02

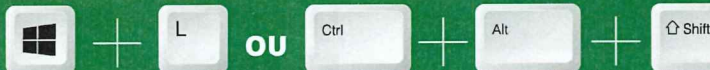
Cette personne pourrait également **accéder au réseau de votre collectivité**, notamment aux espaces de stockages et aux documents de vos collègues.

03

Cette personne **pourrait envoyer des mails, des documents sous votre identité**, et avoir accès à votre carnet d'adresse.

Il est donc essentiel de bien verrouiller son poste dès **que l'on s'éloigne de son ordinateur.**

Pour le faire de manière rapide, vous pouvez utiliser un raccourci clavier



ou





### Une clé USB trouvée ou reçue en cadeau ?



Ne la branchez surtout pas à votre ordinateur professionnel, vous pourriez **mettre en danger vos données et celles de votre collectivité**.



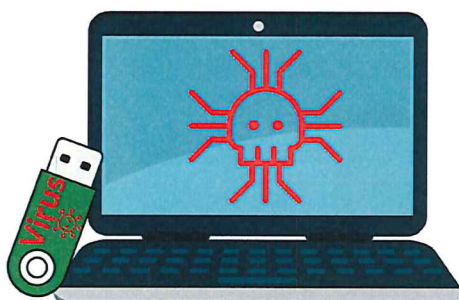
Ne branchez aucun support de stockage USB (Disque dur, Clef usb, Smartphone) **qui n'a pas été contrôlé par votre collectivité** sur votre ordinateur professionnel.



Une clé USB trouvée ou que l'on vous aurait offerte **peut contenir un virus ou être une clé dédiée à l'attaque**, ce qui mettrait en danger toutes nos données (destruction, corruption ou vol).



Faire obligatoirement **contrôler par la DSI** tous les supports de stockage venant d'un environnement non sécurisé par nos soins, même ceux qui ont été fournis par votre collectivité







**Soyez toujours très attentif avant de cliquer sur un lien reçu dans un e-mail !**



En cliquant sans vérifier la validité du lien, vous pourriez vous faire **voler des informations sensibles** ou **compromettre la sécurité de votre poste de travail** et de l'intégralité des données de la collectivité.



Si vous ne prenez pas garde avant de cliquer sur un lien reçu par e-mail, SMS, chat ou tout autre support, vous pourriez être **victime d'un piratage**.



Avant de cliquer, vous devez **prendre le temps de vérifier que le lien est valide** si vous ne voulez pas prendre le risque de diffuser involontairement vos données et celles de votre collectivité à un pirate ou de compromettre la sécurité de votre poste de travail.



En cas de doute, il est toujours préférable **de sélectionner l'URL du site et de la copier/coller** dans votre navigateur (Google Chrome, Mozilla Firefox, Microsoft Edge, Safari).



Ne **jamais consulter ses mails privés** à partir de votre outil de travail. En effet, cela n'est pas sécurisé par notre outil de filtrage.





Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications de la collectivité... la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe.

Face à la profusion des mots de passe, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès.

Voici **10 bonnes pratiques** à adopter pour gérer efficacement vos mots de passe

- 01 Utilisez un mot de passe différent pour chaque applicatif
- 02 Utilisez un mot de passe suffisamment long et complexe.
- 03 Utilisez un mot de passe\* impossible à deviner.
- 04 Utilisez un gestionnaire de mots de passe (Keepass).
- 05 Changez votre mot de passe au moindre soupçon
- 06 Ne communiquez jamais votre mot de passe à un tiers.
- 07 N'utilisez pas vos mots de passe sur un ordinateur partagé.
- 08 Activez la «<double authentification>> lorsque c'est possible
- 09 Changez les mots de passe par défaut des différents services aux quels vous accédez.
- 10 Choisissez un mot de passe particulièrement robuste pour votre messagerie.

\*LA MÉTHODE DES PREMIÈRES LETTRES: Un tiens vaut mieux que deux tu l'auras: ltvMq2tl'A

LA MÉTHODE PHONÉTIQUE: J'ai acheté huit CD pour cent euros cet après-midi : ght8CD%E7am





## IMPORTANT

Je suis  
scrupuleusement les  
consignes de  
télétravail pour ne pas  
exposer d'avantage le  
système informatique  
à des attaques.

# RESPECTER LES RÈGLES DU TÉLÉTRAVAIL

### Recommandations de sécurité pour les télétravailleurs

01

Appliquez strictement les consignes de sécurité de votre collectivité.

02

Ne faites pas en télétravail ce que vous ne feriez pas au bureau.

03

Renforcez la sécurité de vos mots de passe.

04

Sécurisez votre connexion WiFi.

05

Sauvegardez régulièrement votre travail.

06

Méfiez-vous des messages inattendus.

07

N'installez vos applications que dans un cadre << officiel >> et évitez les sites suspects.

08

L'utilisation d'un ordinateur professionnel à des fins personnelles est strictement interdite. En effet, mélanger nos vies professionnelles et privées sur le matériel fournit par la collectivité peut nous porter préjudice, mais également nuire à la collectivité. Notre réseau pourrait subir des cyberattaques.



## IMPORTANT

Je stocke mes données de travail sur les serveurs car ce sont les seuls espaces de stockage sécurisés et sauvegardés

# STOCKER MES FICHIERS SUR LES SERVEURS

## Les avantages du stockage sur le serveur

✓ Idéal pour la **sauvegarde** de gros volumes

✓ Restauration des données simple et ultra rapide

✓ **Intégrité** et récupération des données plus rapide

✓ **Travail collaboratif** de meilleure qualité

✓ **Travail collaboratif** de meilleure qualité

✓ **Sécurité** : les ordinateurs portables sont sujets à de nombreux vols.

Environ 800 000 ordinateurs portables sont volés et/ou perdus chaque année.

Grâce au serveur mis en place au sein de la collectivité, les données restent accessibles dans un dossier partagé ou privé et sauvegardées (puisqu'elles sont centralisées sur un serveur).

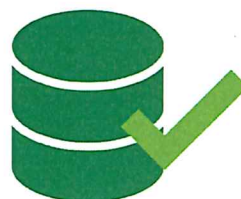
## Les inconvénients du disque dur

✗ Le disque dur peut crasher à tout moment et entraîner la perte de vos fichiers. Cela n'est pas le cas avec du stockage en réseau qui va nous permettre de se prémunir contre ce risque.

✗ Le disque dur qui contient toutes vos données meurt, les informations meurent avec lui!

Lorsque vous stockez des informations localement, vous augmentez le risque de perte de données en cas de vols, d'incendies, d'inondations ou autres incidents.

✗ Le plus grand inconvénient du stockage local est que vos données sont accessibles que par vous et non sauvegardées. Il est compliqué de partager des données avec les membres de votre équipe si vous n'êtes pas tous connectés au réseau local.







Autant de gestes qui vous permettront de maintenir une confidentialité accrue dans votre collectivité et garder la confiance de vos collaborateurs.



Ranger et organiser son bureau



Classer et verrouiller les informations sensibles sur votre ordinateur.



Activer l'économiseur d'écran par mot de passe.



Détruire les post-its ou notes dont les informations peuvent être sensibles.



Étendre la culture «bureau propre» sur ordinateur, appareil mobile, et ranger les documents imprimés, carte d'accès, clef usb, disque dur...







Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise.

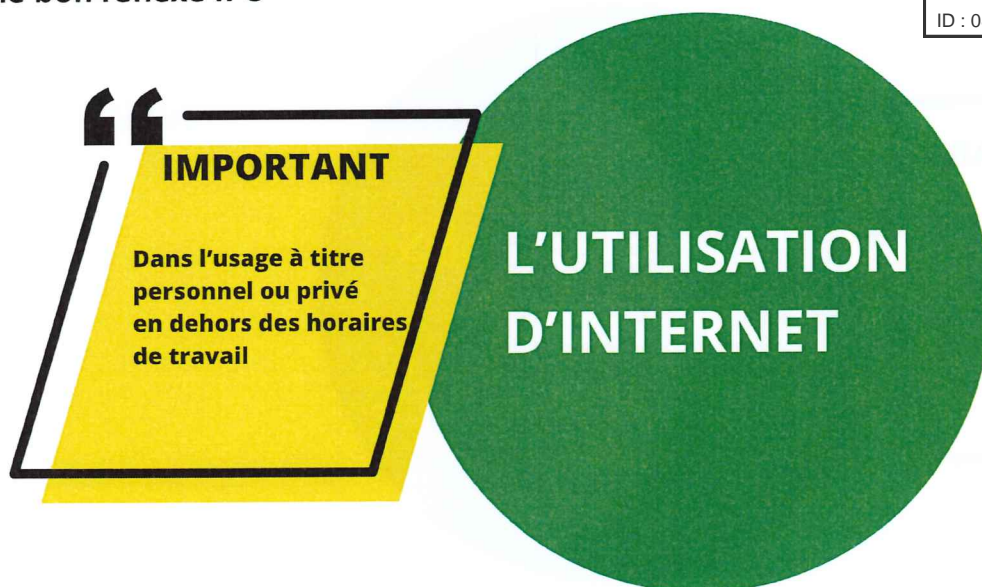
Une personne physique peut être identifiée directement (exemple: nom et prénom).

Les fichiers présents sur votre ordinateur de travail sont supposés être professionnels, sauf si vous les identifiez clairement comme étant personnels

Si vous stockez des documents personnels:

- 01 Rangez-les dans un répertoire ou un dossier intitulé "Personnel" ou "Privé".
- 02 Mettez en évidence les données considérées privées, en faisant figurer "PRIVÉ" en tête du nom, des dossiers, et de l'objet des courriels.
- 03 L'intitulé "Mes documents", vos initiales ou votre prénom ne suffisent pas à lui donner un caractère personnel.



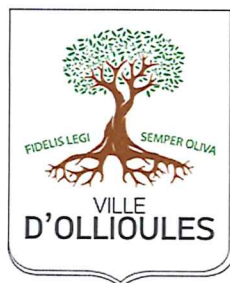


### Usage à titre privé ou personnel :

La mairie tolère une utilisation raisonnable des moyens informatiques de la collectivité à des fins privées ou personnelles, en dehors des horaires de travail, utilisation qui ne porte pas atteinte au bon fonctionnement de la collectivité, au bon fonctionnement des ressources informatiques et à la bonne exécution des missions et dont les modalités sont les suivantes :

- Cette utilisation est limitée aux pc bureautiques, téléphones, internet, mail. Cela exclut notamment les ressources métier et les espaces de stockage centralisés.
- Cette utilisation ne doit pas mettre en danger les applications professionnelles par des comportements à risque ou par une utilisation excessive des ressources disponibles, notamment les ressources de stockage et de bande passante des réseaux.
- Cette utilisation doit être à destination strictement personnelle.
- Cette utilisation doit s'opérer en conformité avec les lois en vigueur. Il est notamment interdit d'utiliser les moyens informatiques de l'entreprise pour effectuer de téléchargements illicites ou accéder à des sites illégaux ou à caractères pornographiques.
- Cette utilisation ne doit pas porter préjudice à l'image de la collectivité.
- Cette utilisation ne doit pas perturber l'activité professionnelle des collaborateurs ou des collègues de l'utilisateur.





## Récépissé de la charte informatique

**Je soussigné(e)**

**Nom :** .....

**Prénom :** .....

**Service :** .....

**Fonction :** .....

Agent de la commune d'Ollioules, déclare avoir pris connaissance de la charte informatique et m'engage à la respecter. Utilisateur des moyens informatiques et réseaux de la collectivité, déclare avoir pris connaissance de la présente charte et m'engage à la respecter.

**Fait à** .....

**Le** .....

Fait en deux exemplaires :

Un pour l'intéressé

Un pour la collectivité

**Signature**



Envoyé en préfecture le 17/04/2024

Reçu en préfecture le 17/04/2024

Publié le

ID : 083-218300903-20240408-D2024\_04\_4\_12-DE