

# Charte informatique de la Médiathèque

## Préambule

La Médiathèque met à disposition de ses utilisateurs un système d'information et des moyens informatiques nécessaires à l'exécution de ses missions et de ses activités.

Dans le cadre de leurs fonctions, les utilisateurs sont conduits à utiliser ces ressources informatiques mises à leur disposition par la Médiathèque.

Dans un esprit de transparence, la présente charte définit les règles d'utilisation de ses ressources au sein de la Médiathèque.

## Article 1 : Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs du système d'information dont notamment :

1

- Le maire et les élus
- Les responsables des services
- Les agents territoriaux (titularisés et non titularisés)
- Les intérimaires
- Les stagiaires

## Article 2 : Périmètre du système d'information

Le système d'information est composé des ressources suivantes :

Celui-ci comprend :

- Un réseau informatique
- Un réseau téléphonique
- Des terminaux informatiques (ordinateurs fixe)
- Des systèmes d'impression et de numérisation (photocopieur, scanner ...)
- Un environnement applicatif de travail : messagerie électronique, logiciels métiers, logiciels de bureautique [...]

Aux fins d'assurer la sécurité informatique du système d'information, tout matériel connecté au système d'information de la collectivité, y compris le matériel personnel des utilisateurs indiqués à l'article 1, est régi par la présente charte.

## Article 3 : Règles générales d'utilisation

Le système d'information doit être utilisé à des fins strictement professionnelles, conformes aux objectifs de l'organisation, sauf exception prévue par les présentes, ou par la loi.

Les utilisateurs ne peuvent en aucun cas utiliser le système d'information de l'organisation pour se livrer à des activités illégales, et/ou susceptibles de porter préjudice à l'organisation de quelque manière que ce soit.

## Article 4 : Sécurité informatique

L'entreprise met en œuvre une série de moyens pour assurer la sécurité de son système d'information et des données traitées, en particulier des données personnelles. A ce titre, elle peut limiter l'accès à certaines ressources.

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

2

### 4.2. Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations, et en particulier des données personnelles, traitées sur le système d'information de la collectivité.

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.

### 4.3. Mots de passe

L'accès aux systèmes d'information ou aux ressources informatiques mises à disposition est protégé par des mots de passe individuels. Ces mots de passe doivent être gardés confidentiels par l'utilisateur afin de permettre le contrôle de l'activité de chacun. Les mots de passe doivent être mémorisés et ne doivent pas être écrits sous quelque forme que ce soit. Ils ne doivent pas être transmis ou confiés à un tiers ou être rendus accessibles. Les identifiants et les mots de passe doivent être saisis lors de chaque accès au système d'information.

Les mots de passe doivent se conformer à la stratégie de mot de passe édictée **[conformément à la politique de sécurité de la collectivité/ conformément aux**

prescriptions de l'ANSSI relativement à la protection des données personnelles et notamment :

- Utilisez un mot de passe unique pour chaque application. En particulier, l'utilisation d'un même mot de passe entre sa messagerie professionnelle et sa messagerie personnelle est impérativement à proscrire ;
- Choisissez un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom de société, d'une date de naissance, etc.) ;
- Ne demandez jamais à un tiers de générer pour vous un mot de passe ;
- Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent ;
- Renouvelez vos mots de passe avec une fréquence raisonnable. [Tous les 90 jours] est un bon compromis pour les systèmes contenant des données sensibles ;
- Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur Internet), encore moins sur un papier facilement accessible ;
- Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle ;
- Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.
- Configurez vos mots de passe de façon rigoureuse en respectant une composition de plus de 12 caractères, mêlant majuscules, minuscules, chiffres, caractères spéciaux.]

3

#### 4.4. Verrouillage de sa session

L'utilisateur doit veiller à verrouiller sa session dès lors qu'il quitte son poste de travail.

#### 4.5. Installation de logiciels

L'utilisateur ne doit pas installer, copier, modifier ou détruire des logiciels sur son poste informatique sans l'accord préalable et systématique du **service informatique**.

#### 4.6. Copie de données informatiques

L'utilisateur doit respecter les procédures définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité, afin d'éviter la perte de données (*ex : vol de clé USB, perte d'un ordinateur portable contenant d'importantes quantités d'informations confidentielles.* ).

## Article 5 : Modalités spécifiques d'utilisation des ressources informatiques

### 5.1. Accès à internet

L'accès à l'internet est autorisé au travers du système d'information, toutefois, pour des raisons de sécurité l'accès à certains sites peut être limité.

### 5.2. Messagerie électronique

Chaque utilisateur peut disposer d'une ou plusieurs adresse(s) email pour l'exercice de ses missions.

Par principe, tous les messages envoyés ou reçus sont présumés être envoyés à titre professionnel.

Tout message envoyé ou reçu depuis votre messagerie professionnelle est supposé avoir un caractère professionnel, sauf s'il est clairement identifié comme étant personnel (par exemple, avec l'indication "Personnel" ou "Privé" en objet) ou classé dans un répertoire "Personnel".

4

## [Article 6 : Contrôle de l'usage]

**NOTE : la collectivité peut édicter ses propres règles pour procéder à la distinction des usages privés et professionnels en fonction de son système d'information, toutefois il est impossible de supprimer un usage raisonnable à titre privé des outils informatiques mis à disposition par l'employeur, elle doit donc nécessairement édicter des règles à ce titre.**

## Article 7 : Sanctions

Les manquements aux règles édictées par la présente charte peuvent engager la responsabilité de l'utilisateur et entraîner des sanctions à son encontre.

Tout utilisateur du système d'information de la collectivité n'ayant pas respecté la loi, pourra être poursuivi pénalement.

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.

## Article 8 : Information et entrée en vigueur

La présente charte est visée par chaque utilisateur de la collectivité et ajoutée en annexe du règlement intérieur.

Elle entre en vigueur au ...

Fait à ....., le .....

Signature du représentant de la collectivité