Version du 24/03/2016

# CHARTE INFORMATIQUE

## PREAMBULE

La Mairie de Maurepas met en œuvre un Système d'Information et de Communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des outils mobiles.

Les agents, dans l'exercice de leurs fonctions, sont conduits à utiliser les outils informatiques et téléphoniques mis à leur disposition et à accéder aux services de communication de la Mairie.

L'utilisation du système d'information et de communication doit se faire exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et de communication, la présente charte pose les règles relatives à l'utilisation de ces ressources. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, non seulement pour la bonne exécution du contrat de travail des agents, mais aussi dans le cadre de la responsabilité pénale et civile de l'employeur.

Elle dispose d'un aspect réglementaire et est annexée au règlement intérieur de la Mairie. Elle ne remplace en aucun cas les lois en vigueur que chacun est censé connaître.

## 1) CHAMP D'APPLICATION

### 1) UTILISATEURS CONCERNES

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de la Mairie, quel que soit leur statut, y compris les élus, agents, vacataires, stagiaires, employés de sociétés prestataires, visiteurs occasionnels. Elle sera annexée aux contrats de prestations.

Les agents veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

### 2) SYSTEME D'INFORMATION ET DE COMMUNICATION

Le système d'information et de communication de la Mairie est notamment constitué des éléments suivants: ordinateurs (fixes ou portables), périphériques y compris clés USB délivrées par la DSI, réseau informatique (serveurs, routeurs et connectique), photocopieurs, télécopieurs, téléphones, smartphones, tablettes et clés 3G/4G, logiciels, fichiers, données et bases de données, système de messagerie, connexion internet, intranet, extranet, abonnements à des services interactifs.

**Pour des raisons de sécurité du réseau et des données, aucun matériel personnel quel qu'il soit (clé, disque dur, téléphone portable, ordinateur, imprimante, webcam, etc.) ne peut être connecté au réseau de la Mairie.**

### 3) AUTRES ACCORDS SUR L'UTILISATION DU SYSTEME D'INFORMATION

La présente charte ne préjuge pas des accords particuliers pouvant porter sur l'utilisation du système d'information et de communication par les institutions représentatives, l'organisation d'élections par voie électronique ou la mise en télétravail d'agents.

## 2) CONFIDENTIALITE

### 1) PARAMETRES D'ACCES

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe).

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs.

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres des mots de passe doivent respecter un certain degré de complexité (au moins 8 caractères dont au moins 1 majuscule, 1 minuscule, 1 chiffre) et être modifiés tous les 6 mois. Des consignes de sécurité sont élaborées par la DSI afin de recommander les bonnes pratiques en la matière. Sauf demande formelle de la Direction Générale, aucun utilisateur ne doit se servir pour accéder au système d'information de la Mairie d'un autre compte que celui qui lui a été attribué. Il ne doit pas non plus déléguer à un tiers les droits d'utilisation qui lui sont attribués.

Chaque utilisateur est responsable en ce qui le concerne du respect du secret professionnel et la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Les règles de confidentialité ou d'autorisation applicables quel que soit le support de communication utilisé.

L'utilisateur doit être conscient et particulièrement vigilant sur le risque de divulgation de ces informations dans le cadre d'utilisation d'outils informatiques, personnels ou appartenant à la Mairie, dans des lieux autres que ceux de la Mairie (formation, autres collectivités, domicile, lieux publics…).

## 3) SECURITE

### 1) ROLE DE LA COLLECTIVITE

La collectivité met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. À ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

La DSI est responsable de la mise en œuvre et du contrôle du bon fonctionnement du système d'information et de communication. Elle doit prévoir un plan de sécurité et de continuité du service, en particulier en cas de défaut matériel. Elle veille à l'application des règles de la présente charte. Elle est assujettie à une obligation de confidentialité sur les informations qu'elle est amenée à connaître.

### 2) RESPONSABILITE DE L'UTILISATEUR

L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence et de vigilance. En particulier, il doit signaler à la DSI toute violation ou tentative de violation de l'intégrité de ces ressources, et, de manière générale tout dysfonctionnement, incident ou anomalie.

**Sauf autorisation expresse de la DSI, l'accès au système d'information avec du matériel n'appartenant pas à la Mairie (supports amovibles, téléphones personnels…) est interdit**. Dans le cas où il a été autorisé, il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité.

De même, la sortie de matériel appartenant à la Mairie doit être justifiée par des obligations professionnelles et nécessite l'accord exprès de la DSI.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

L'utilisateur doit effectuer des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition en suivant les procédures définies par la DSI. Il doit régulièrement supprimer les données devenues inutiles sur les espaces communs du réseau ; les données anciennes mais qu'il souhaite conserver doivent être archivées avec l'aide de la DSI.

L'utilisateur n'est pas autorisé à installer ou à supprimer des logiciels, à copier ou à installer des fichiers susceptibles de créer des risques de sécurité au sein de la Mairie. Il ne doit pas non plus modifier les paramétrages de son poste de travail ou des différents outils mis à sa disposition, ni contourner aucun des systèmes de sécurité mis en œuvre pour la Mairie.

**En cas de doute, il doit dans tous les cas alerter la DSI.**

L'utilisateur s'oblige en toutes circonstances à se conformer à la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables.

Il ne doit en aucun cas se livrer à une activité concurrente aux services proposés par la Mairie ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.

## 4) INTERNET

### 1) ACCES AUX SITES

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par la DSI qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites.

En particulier, l'utilisation de l'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite. Il est aussi prohibé de créer ou mettre à jour au moyen de l'infrastructure de la Mairie tout site Internet, notamment des pages personnelles.

**Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée.**

Bien sûr, il est interdit de se connecter à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de la Mairie de Maurepas, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de la Mairie de Maurepas ou engageant financièrement celle-ci.

### 2) CAS DE L'UTILISATION DES ORDINATEURS PORTABLES PROFESSIONNELS

Dans le cas d'un ordinateur portable professionnel, l'accès à internet est autorisé sous couvert des bonnes pratiques décrites dans le paragraphe ci-dessus. L'utilisateur doit néanmoins être conscient que toute infection de son ordinateur portable professionnel en dehors du domaine de Maurepas, pourrait nuire gravement au bon fonctionnement du système d'information de la collectivité. Il engagera donc sa responsabilité et devra avertir la DSI si toutefois il supposait que son portable puisse avoir subi une quelconque infection et ce, avant toute reconnexion au réseau professionnel.

D'autre part, le plus grand soin devra être apporté au matériel mobile mis à disposition des utilisateurs (PC portable, tablette, téléphone, etc.). La DSI devra immédiatement être informée de toute anomalie ou dysfonctionnement. En cas de perte ou de casse, une déclaration écrite devra être faite auprès de la direction générale. **Dans tous les cas, un matériel ne pourra être rendu à la DSI sans avoir au préalable été physiquement nettoyé.**

### 3) AUTRES UTILISATIONS

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, chats, blogs n'est autorisée qu'à titre professionnel et sur autorisation expresse de la hiérarchie qui devra en informer la DSI.

De même, tout téléchargement de fichier, en particulier de fichier média, est prohibé, sauf justification professionnelle dûment validée par la hiérarchie.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte à l'image de la Mairie de Maurepas.

Ils sont informés que la DSI pourra enregistrer leur activité sur Internet et que ces traces pourront être exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi, en particulier en cas de perte importante de bande passante sur le réseau de la Mairie.

## 5) MESSAGERIE ELECTRONIQUE

Un nombre défini d'agents disposent, dans le cadre de l'exercice de leur activité professionnelle, d'une adresse de messagerie électronique normalisée attribuée par la DSI. Cette messagerie est accessible aussi bien à partir d'un logiciel de messagerie qu'à partir d'un navigateur Internet grâce à un Webmail.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les agents sont invités à informer la DSI des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

## 1) CONSEILS GENERAUX

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier postal : il obéit donc aux mêmes règles, en particulier en matière d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à son supérieur.

Un message électronique peut être communiqué très rapidement à des tiers et il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de la Mairie de Maurepas et de l'utilisateur.

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, ces vérifications doivent être renforcées.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

En cas d'envoi à une liste de diffusion, il est important de contrôler la liste des abonnés.

Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants doivent être envoyés avec un accusé de réception.

Ils doivent, le cas échéant, être doublés par un envoi de fax ou de courrier postal.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent pas comporter d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

La forme des messages professionnels doit respecter les règles définies par la Direction Générale, pour ce qui concerne la mise en forme, la charte graphique et surtout la signature des messages.

En cas d'absence supérieure à 3 jours, l'agent doit mettre en place un répondeur automatique.

## 2) LIMITES TECHNIQUES

Pour des raisons techniques, la DSI est aussi chargée de l'ouverture, de la modification ou de la suppression des listes de diffusion.

La DSI peut limiter la taille, le nombre et le type des pièces jointes pour éviter l'engorgement du système de messagerie.

Pour des raisons de capacité mémoire, les messages électroniques sont conservés sur le serveur de messagerie pendant une durée maximale de deux ans. Passé ce délai, ils sont automatiquement supprimés. Si l'agent souhaite conserver des messages au-delà de ce délai, il lui appartient d'en faire des sauvegardes avec l'aide de la DSI si nécessaire.

Il est aussi tenu de supprimer lui-même dès que possible tous les messages inutiles et notamment ceux comportant des pièces jointes supérieures à 1 méga.

### 3) UTILISATION PERSONNELLE DE LA MESSAGERIE

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

Les messages envoyés doivent être signalés par la mention "Privé" ou "Perso" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon. Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Perso". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de la Mairie de Maurepas.

### 4) UTILISATION DE LA MESSAGERIE PAR LES REPRESENTANTS DU PERSONNEL

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel, mais en utilisant la mention "Syndicat" dans leur objet à l'émission et dans le dossier où ils doivent être classés.

Les représentants du personnel disposent d'une adresse de messagerie dédiée à leur mission. Pour des raisons d'identification et de sécurité, il est fortement conseillé d'utiliser ces boîtes mails. Dans le cas où cette instance représentative utiliserait une adresse mail étrangère au nom de domaine « maurepas.fr » , elle engagerait sa responsabilité en cas d'attaque virale avérée.

## 6) TELEPHONIE

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un poste fixe et d'un terminal mobile, smartphone, tablette ou clé 3/4G.

Pour ce qui est de l'utilisation des smartphones en connexion pour accès à des sites Internet ou à la messagerie électronique, les règles édictées ci-dessus s'appliquent de la même manière.

De plus, il est rappelé que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel. Il est donc soumis aux mêmes règles rappelées plus haut.

Enfin, les connexions depuis l'étranger sont strictement interdites sauf autorisation exceptionnelle de la Direction Générale en cas d'urgence professionnelle.

### A) UTILISATION PERSONNELLE DE LA TELEPHONIE

L'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites raisonnables en termes tant de temps passé que de quantité d'appels.

Les surcoûts pour la collectivité, engendrés par l'utilisation de la téléphonie à des fins personnelles devront être remboursés par les utilisateurs concernés. Il s'agit tout particulièrement des appels à des numéros surtaxés et des appels depuis l'étranger ou à destination de l'étranger, au sens de la facturation téléphonique.

Les utilisateurs sont informés que la DSI enregistre leur activité téléphonique, aussi bien sur les postes fixes que sur les mobiles. Ces traces seront exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi. Toutefois, seule la Direction Générale pourra avoir accès aux numéros détaillés, permettant d'identifier les interlocuteurs d'un utilisateur, et seulement en cas de différend avec lui.

## 7) DONNEES PERSONNELLES

La loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, définit les conditions dans lesquelles des traitements de données personnelles peuvent être opérés. Elle institue au profit des personnes concernées par les traitements des droits que la présente invite à respecter, tant à l'égard des utilisateurs que des tiers.

Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle, prévus dans la présente charte. Ils sont, en tant que de besoin, déclarés conformément à la loi du 6 janvier 1978. Tout utilisateur pourra avoir accès aux données le concernant et ces données ne seront conservées que sur une période maximale de 1 an.

Il est rappelé aux utilisateurs que les traitements de données à caractère personnel doivent être déclarés à la Commission nationale de l'informatique et des libertés, en vertu de la loi n° 78-17 du 6 janvier 1978. Les utilisateurs souhaitant réaliser, dans le cadre professionnel, des traitements relevant de ladite loi sont invités à prendre contact avec la DSI avant d'y procéder.

## 8) ABSENCE DE L'AGENT

En cas d'absence de l'agent, la continuité du service doit être assurée. L'agent doit donc veiller à ce que son service puisse accéder aux documents, logiciels et dossiers indispensables à l'activité (transmission des documents et dossiers aux collègues, ou mise à disposition dans un dossier partagé, création de comptes pour accéder aux applications, à l'exclusion de toute communication de mots de passe personnels). Si l'absence est imprévue (maladie, accident), le supérieur hiérarchique pourra demander au service informatique l'accès à l'espace de travail de l'agent. En cas de départ définitif ou de mutation, l'agent est seul habilité à récupérer ou sauvegarder les documents et messages privés. Le successeur quant à lui, récupère les documents de travail ainsi que les messages d'ordre professionnel. Enfin, l'adresse email attribuée à l'utilisateur est automatiquement détruite 30 jours après son départ sans qu'aucune sauvegarde ne soit effectuée.

# 9) CONTROLE DES ACTIVITES

## 1) CONTROLES AUTOMATISES

Le système d'information et de communication s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de la Mairie, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication.

Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers,
- aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites ou le téléchargement de fichiers,
- aux appels téléphoniques émis ou reçus à partir des postes fixes ou mobiles pour surveiller le volume d'activités et détecter des dysfonctionnements.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

Il est précisé que chaque utilisateur pourra avoir accès aux informations enregistrées lors de ces contrôles le concernant sur demande préalable à la Direction Générale.

De plus, les fichiers journaux énumérés ci-dessus sont automatiquement détruits dans un délai maximum de 6 mois après leur enregistrement.

## 2) PROCEDURE DE CONTROLE MANUEL

En cas de dysfonctionnement constaté par la DSI, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Le contrôle concernant un utilisateur peut porter sur les fichiers contenus sur le disque dur de l'ordinateur, sur un support de sauvegarde mis à sa disposition ou sur le réseau de la Mairie de Maurepas, ou sur sa messagerie. Alors, sauf risque ou événement particulier, la Direction Générale ne peut ouvrir les fichiers ou messages identifiés par l'utilisateur comme personnels ou liés à la délégation de personnel conformément à la présente charte, qu'en présence de l'utilisateur ou celui-ci dûment appelé et éventuellement représenté par un délégué du personnel.

## 10) INFORMATION ET SANCTIONS

La présente charte est accessible sur l'intranet de la ville et remise à l'agent nouvellement recruté. Un exemplaire est également consultable dans chaque direction. Une fiche de synthèse reprenant les principaux éléments de cette charte devra être signée par chaque agent.

La DSI est à la disposition des agents pour leur fournir toute information concernant l'utilisation du système d'information, en particulier sur les procédures de sauvegarde et de filtrage. Elle les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication ainsi que sur les menaces susceptibles de peser sur sa sécurité.

Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la DSI dans le cadre de la présente charte. En cas de besoin, les agents pourront être formés par la DSI pour appliquer les règles d'utilisation du système d'information et de communication prévues.

Le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Dans ce dernier cas, les procédures prévues dans le règlement intérieur article 9ème (sanctions disciplinaires) et dans le statut général des fonctionnaires de l'état et des collectivités territoriales seront appliquées.

L'utilisation reconnue à des fins personnelles de certains services payants à travers le système de communication de la Mairie de Maurepas donnera également lieu à remboursement de la part de l'utilisateur concerné.

## 11) ENTREE EN VIGUEUR

La présente charte est applicable à compter du 1er novembre 2016

Elle a été adoptée après information et consultation du CT en date du 05 avril 2016.