

**MISE À JOUR : 09.2024**

**- MODELE -**

**CHARTE D’UTILISATION DES SYSTEMES D’INFORMATION**

**proposé aux collectivités affiliées**

**au Centre de Gestion de la Manche**

**Chaque collectivité doit adapter ce modèle à sa propre situation**, en fonction des services et des installations dont elle dispose et solliciter l’avis du comité social territorial (CST), avant son adoption définitive par délibération de l’assemblée délibérante. Une fois adopté, la charte informatique devient force réglementaire dans la collectivité.

**SOMMAIRE**

[LEXIQUE 3](#_Toc167202932)

[PREAMBULE 4](#_Toc167202933)

[1. Définition et objectifs 4](#_Toc167202934)

[2. Champ d’application de la charte 4](#_Toc167202935)

[UTILISATION DES OUTILS INFORMATIQUES 5](#_Toc167202936)

[1. Protection des données 5](#_Toc167202937)

[1.1. Données professionnelles 5](#_Toc167202938)

[1.2. Données privées 5](#_Toc167202939)

[2. Internet 6](#_Toc167202940)

[3. Wifi 6](#_Toc167202941)

[4. Fonctionnement optimal des outils informatiques 6](#_Toc167202942)

[UTILISATION DES OUTILS DE COMMUNICATION 7](#_Toc167202943)

[1. Messagerie 7](#_Toc167202944)

[1.1. Messages professionnels 7](#_Toc167202945)

[1.2. Messages privés 7](#_Toc167202946)

[1.3. Fonctionnement optimal de la messagerie 8](#_Toc167202947)

[2. Téléphonie 8](#_Toc167202948)

[ENGAGEMENTS DE LA COLLECTIVITE 8](#_Toc167202949)

[1. Responsabilités de l’employeur 8](#_Toc167202950)

[2. Données nominatives - RGPD 9](#_Toc167202951)

[DEPART D’UN UTILISATEUR 10](#_Toc167202952)

[SANCTIONS DE L’UTILISATEUR 10](#_Toc167202953)

[PRET DE MATERIELS 10](#_Toc167202954)

[RECEPISSE DE LA CHARTE D’UTILISATION DU SYSTEME D’INFORMATION 11](#_Toc167202955)

Code Général de la Fonction Publique

Code pénal, notamment les articles 121-2, 226-15, 323-1 et suivants

Code civil, notamment l’article 1384

Code de la propriété intellectuelle, notamment les articles L.111-1 et suivants, L.112-2, L.113-9, L.122-6 et   
L.122-6-1, L.332-4, L.335-3 et L.336-6

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Cour de cassation, Chambre sociale, 2 octobre 2001, n°99-42.942

Cour de cassation, Chambre sociale, 9 juillet 2008, n°06-45.800

Cour d'appel de Colmar, 29 mai 2008, n°07/03314

Cour d'appel de Rennes, 14 janvier 2010, n°08/02209

# LEXIQUE

**« employeur »**: Maire/Président, employeur des agents de la collectivité. La direction pourra être dépositaire de l’autorité publique, pour exercer le rôle d’employeur. Les administrateurs pourront les assister dans le rôle qui leur est dévolu dans la présente charte.

**« utilisateur »** : toute personne (élu, agent fonctionnaire ou contractuel, prestataire externe, stagiaire, temporaire…) ayant accès ou utilisant les ressources informatiques mises à disposition par la collectivité.

**« outils informatiques »**:

* Le poste de travail
* Le réseau
* Internet et extranet
* La tablette…

**« outils de communication »**:

* La messagerie
* Le téléphone
* Le télécopieur
* Le smartphone…

**« administrateurs »**: les membres de l’équipe informatique, stagiaires compris.

**« données nominatives » :** toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

# PREAMBULE

## Définition et objectifs

Les agents de la collectivité utilisent quotidiennement des outils informatiques et de communication nécessaires au bon déroulement de leurs missions.

La présente charte a pour objet d’informer les utilisateurs des modalités d’utilisation de ces outils dans les meilleures conditions possibles, tant en termes de fonctionnement des services que de légalité.

Elle vise non seulement à donner le cadre d’une bonne utilisation des outils informatiques, tels que les logiciels de bureautique, les outils de création et de gestion des images, Internet, mais aussi à définir le bon usage du réseau, du stockage des données, ou encore l’utilisation des périphériques externes.

Elle a également pour finalité de contribuer à la préservation de la sécurité du système d’information de la collectivité.

Elle expose les principales obligations que tout utilisateur doit respecter et mettre en œuvre dans l’utilisation du système d’information mis à sa disposition dans le cadre de l’exercice de ses missions.

Chaque utilisateur doit être conscient que :

* l’usage du système d’information obéit à des règles qui s’inscrivent dans le respect de la loi, de la déontologie et de la sécurité de la collectivité,
* l’ouverture d’un réseau informatique constitue toujours un risque pour la sécurité,
* la négligence ou la mauvaise utilisation de ces ressources fait courir des risques à la collectivité, aux agents, aux élus, et aux usagers.

Tout utilisateur contribue donc à la sécurité générale du système d’information. A cette fin, l’utilisateur est informé par la présente charte des règles d’utilisation et de fonctionnement, ainsi que des sanctions encourues en cas de non-respect de la présente charte.

Elle a été soumise à l’avis du Comité Social Territorial du Centre de Gestion de la Manche en date du à préciser et sera portée à la connaissance de chacun des utilisateurs.

## Champ d’application de la charte

La présente charte s'applique à l’ensemble des utilisateurs du système d’information de la collectivité, tous statuts confondus, ainsi qu’aux agents temporaires, apprentis, stagiaires et élus, que l’utilisateur soit en présentiel ou en télétravail.

Elle s’applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques de la collectivité.

L’ensemble des dispositions sont applicables aux utilisateurs accédant à distance aux systèmes d’information et de communication de la collectivité, en utilisant le matériel fourni par la collectivité pour accéder à l’architecture du système informatique. Tout accès à distance par du matériel informatique personnel est interdit, sauf autorisation préalable.

Les moyens informatiques et outils numériques susceptibles d’être mis à disposition des utilisateurs sont les suivants :

**☞ A COMPLETER**

Exemples :

* Postes informatiques :
* Matériels : ordinateur fixe, ordinateur portable, écrans, clavier, souris…
* Système d’exploitation : Windows
* Logiciel : pack bureautique, antivirus, applications spécifiques
* Imprimantes simples ou multifonctions
* Tablettes
* Téléphones fixes, smartphones, accessoires (casques notamment)
* Messageries électroniques, accès à Internet, Extranet
* Réseau informatique et de télécommunication, serveurs, systèmes de sécurité et de collecte des données
* Système d’information au sens large, dont logiciels, applications métiers, GED, données (numériques, images, sons) et échanges de fichiers…

# UTILISATION DES OUTILS INFORMATIQUES

## Protection des données

### Données professionnelles

1. **Identifiant et mot de passe**

Les utilisateurs qui ont accès au réseau informatique bénéficient d’un droit d’accès par l’utilisation d’un identifiant et d’un mot de passe. Ceux-ci ont pour objectif de préserver la confidentialité des informations professionnelles.

Pour une sécurité optimale des données, la complexité des mots de passe est définie selon les recommandations en vigueur de la CNIL et de l’ANSSI. Après plusieurs échecs de connexion, le compte sera verrouillé. L’utilisateur devra contacter l’administrateur afin qu’il procède à une réinitialisation du mot de passe.

Les identifiants et mots de passe sont par définition personnels ; ils ne pourront être cédés que par la volonté de son bénéficiaire qui en assume alors toute la responsabilité. Pourra dès lors être sanctionnée l’usurpation d’identité d’un autre utilisateur ou l’obtention d’un mot de passe d'un autre utilisateur sans son autorisation.

L’employeur peut néanmoins demander à l’utilisateur de communiquer aux administrateurs ses mots de passe, s’il est absent, et que cela est nécessaire à la continuité du service public. Si l’utilisateur n’est pas en mesure de les fournir, une demande écrite et motivée de son supérieur hiérarchique devra être adressée aux administrateurs.

Afin de protéger les données professionnelles, l’utilisateur doit verrouiller la session de son poste lors de toute absence (même très temporaire) de son bureau. Pour pallier tout oubli, un verrouillage automatique des sessions Windows en cas de non-activité (au bout de 5 minutes) est mis en place.

De plus, chaque utilisateur dispose d’un identifiant et d’un mot de passe personnel pour accéder aux applications le nécessitant.

1. **Réseau**

Pour une préservation des données professionnelles, tout utilisateur s’engage :

* à stocker tout contenu professionnel dans les répertoires communs prévus à cet effet. Si un document de travail doit faire l’objet d’une confidentialité plus stricte que celle définie par les droits d’accès existants, l’utilisateur peut prendre contact avec un administrateur afin qu’il crée un répertoire assorti de droits spécifiques,
* à ne pas altérer les données ou accéder à des informations appartenant à d'autres utilisateurs, sans leur autorisation,
* à ne pas modifier ou détruire des ressources connectées au réseau sans autorisation des administrateurs ou d’un supérieur hiérarchique, ou a minima sans s’être assuré que ces ressources ne sont pas utilisées par d’autres utilisateurs.

### Données privées

Tous les fichiers ou dossiers enregistrés sur les outils informatiques sont présumés professionnels.

Néanmoins, une utilisation à titre privé des outils informatiques est admise, dès lors qu’elle est raisonnable et qu’elle ne nuit pas au bon fonctionnement du service.

Les dossiers doivent contenir les mentions « privé » ou « perso » dans leur nom pour pouvoir être protégés par le droit au respect de la vie privée des utilisateurs. Les fichiers personnels peuvent être stockés uniquement sur le disque dur de l’ordinateur.

## Internet

L'utilisation d'Internet, quel qu’en soit le support (ordinateur, smartphone, tablette…) est réservée à des fins professionnelles et/ou syndicales dans le cadre de l'exercice des décharges d'activité et autorisations spéciales d'absence.

Néanmoins, il est toléré un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel et ne détourne pas l’utilisateur de ses objectifs de travail.

L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine, notamment la pédopornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée.

Sont strictement interdits :

* le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires...),
* le stockage permanent sur les postes de données téléchargées sur Internet,
* le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet.

Tout abonnement payant à un site web ou à un service via Internet doit faire l'objet d'une autorisation préalable du Maire/Président.

Pour éviter les abus et en cas de doute légitime, le Maire/Président peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites les plus visités.

Toute saisie d'informations sur un site Internet professionnel nécessite l'autorisation préalable du Maire/Président.

L'utilisation des réseaux sociaux et des forums de discussion sont autorisées pour un usage professionnel.

## Wifi

À l’intérieur des locaux de la collectivité, l’utilisateur d’un ordinateur portable mis à disposition par la collectivité doit se connecter au réseau local via le câble et la prise réseau informatique.

Le Wifi « préciser le nom de ce wifi » est exclusivement réservé aux agents de la collectivité lors de l’utilisation des salles de réunions. Il est sécurisé par un mot de passe, qui ne doit en aucun cas être communiqué à une personne extérieure à la collectivité.

Le Wifi « préciser le nom de ce wifi » est accessibles aux élus de la collectivité et aux personnes extérieures qui souhaitent se connecter à Internet.

## Fonctionnement optimal des outils informatiques

Afin de permettre un fonctionnement optimal du poste de travail et d’éviter tout dysfonctionnement technique, tout utilisateur s’engage :

* à ne pas télécharger ou installer tout logiciel ou mise à jour non validés par un administrateur,
* à ne pas désactiver les systèmes de protection de son poste de travail,
* à ne pas interrompre, sans y être autorisé, le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau,
* à ne pas brancher de supports numériques (clé USB, carte SD, téléphone portable, disque externe) autres que ceux fournis par un administrateur ou un responsable, sans en avoir fait la demande auprès des administrateurs, exception faite pour le transfert de photos d'un appareil photo,
* à signaler aux administrateurs tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de fonctionnement anormal et de façon plus générale toute atteinte à la sécurité et manquement substantiel à cette charte.

L'ensemble des données saisies et mises en forme par l'utilisateur dans le cadre de ses missions appartient à la collectivité. Selon leur finalité, tous les fichiers de l'utilisateur peuvent être partagés dans le cadre de l'organisation de la collectivité afin d'assurer la continuité du service public.

L'utilisateur est informé des contraintes de confidentialité inhérentes à la communication à des tiers des données ou fichiers appartenant à la collectivité, et de la nécessité de vérifier, avant tout partage, l'habilitation des destinataires.

Afin de protéger la confidentialité des données à caractère personnel, les documents en contenant doivent être immédiatement récupérés après une impression.

Le respect de la confidentialité peut être garanti par l’utilisation de la fonctionnalité « impression privée » qui permet de lancer des impressions et de les récupérer ultérieurement en tapant un code PIN sur le photocopieur. De plus, l’utilisation de cette fonctionnalité permet de garantir la récupération des impressions réalisées sans surcharger la pièce copieur de documents non utilisés ou encore d’éviter que des impressions ne soient emportées par un autre utilisateur.

De plus, la prévention et la résolution de problèmes techniques autorisent les administrateurs à analyser un certain nombre d’éléments relatifs aux flux de trafic et aux volumes stockés (voir partie « ENGAGEMENTS DE LA COLLECTIVITE »).

# UTILISATION DES OUTILS DE COMMUNICATION

## Messagerie

### Messages professionnels

Les échanges électroniques avec des tiers ont la même valeur juridique que les échanges écrits. Un message électronique peut donc être une preuve ou un début de preuve, engageant l’utilisateur ou l’employeur, au même titre qu’un courrier écrit.

Il est donc conseillé de conserver tous les messages, envoyés ou reçus, qui peuvent avoir une valeur contractuelle ou une valeur juridique pertinente (par exemple : engagement sur une prestation, conseil sur un dossier sensible, procédure de marché public…).

Par ailleurs, tout utilisateur s’engage à ne pas masquer son identité, ni diffuser des informations confidentielles relatives à la collectivité, à ses usagers, co-contractants et partenaires ou aux agents, sauf si la conduite des dossiers ou le droit à l’information le requiert.

En son absence, tout utilisateur est censé avoir pris les dispositions nécessaires pour assurer la continuité du service public (par exemple : gestionnaire d’absence de messagerie indiquant les contacts des suppléants). A cet effet, les administrateurs peuvent, ponctuellement, transférer au supérieur hiérarchique de l’utilisateur un message électronique, reçu par ce dernier, identifié comme ayant un caractère professionnel par son objet et/ou son expéditeur.

Le supérieur hiérarchique n'a pas accès aux autres messages de l’utilisateur absent. Celui-ci est informé dès que possible de la liste des messages qui ont été transférés. En cas d’absence prolongée, le supérieur hiérarchique peut demander aux administrateurs, après accord du Maire/Président/Directeur…, le transfert des messages reçus. Néanmoins, de façon exceptionnelle, l’employeur peut être amené à accéder à la messagerie de l’utilisateur en son absence, lorsque cela est nécessaire à la continuité du service public.

### Messages privés

Toute utilisation des moyens de communication est présumée professionnelle.

Néanmoins, une utilisation à titre privé des moyens de communication est admise, dès lors qu’elle est raisonnable et qu’elle ne nuit pas au bon fonctionnement du service.

Les messages doivent contenir les mentions « privé » ou « perso » dans leur objet pour pouvoir être protégés par le droit au respect de la vie privée des agents et du secret des correspondances.

### Fonctionnement optimal de la messagerie

Afin de ne pas provoquer de dysfonctionnements de sa messagerie, et plus globalement, de l’ensemble des messageries de la collectivité, tout utilisateur s’engage :

* à supprimer rapidement tous les messages volumineux et sans valeur juridique pertinente, le volume des boites et des messages échangés étant limité,
* à archiver régulièrement la base de messagerie,
* à avertir les administrateurs de la réception de mails suspects (objet douteux, provenance d’un émetteur inconnu, pièce jointe non habituelle...), afin qu’ils procèdent à leur analyse et/ou suppression.

Tout dysfonctionnement doit être signalé aux administrateurs qui en rendront compte à l’employeur, pour prendre les mesures correctives et préventives.

De plus, la prévention et la résolution de problèmes techniques autorisent les administrateurs à analyser un certain nombre d’éléments relatifs aux flux de trafic et aux volumes stockés (voir partie « ENGAGEMENTS DE LA COLLECTIVITE »).

## Téléphonie

L'utilisation des téléphones fixes et portables est réservée à des fins professionnelles.

Néanmoins, un usage ponctuel du téléphone pour des communications personnelles locales est toléré pour des besoins impérieux et à condition que cela n'entrave pas l'activité professionnelle.

L'utilisation des téléphones portables personnels doit rester occasionnelle et discrète.

En cas d'absence, l'utilisateur doit effectuer un renvoi de sa ligne fixe sur le poste d’un autre utilisateur de son service ou à l'accueil.

Le Maire/Président peut procéder au contrôle de l'ensemble des appels émis via les téléphones professionnels.

La collectivité s’interdit de mettre en œuvre un suivi individuel systématique de l’utilisation des services de télécommunications. Seules des statistiques globales peuvent être réalisées sur l’ensemble des appels entrants et sortants.

La collectivité vérifie que les consommations n’excèdent pas les limites des contrats passés avec les opérateurs. Elle s’interdit d’accéder à l’intégralité des numéros appelés via l’autocommutateur mis en place et via les téléphones portables. Toutefois, en cas d’utilisation manifestement anormale, les administrateurs, sur demande du Maire/Président/de la direction, se réservent le droit d’accéder aux numéros complets des relevés individuels.

# ENGAGEMENTS DE LA COLLECTIVITE

## Responsabilités de l’employeur

L’employeur est responsable des faits commis par ses agents au moyen de ses outils informatiques et de communication.

Pour une utilisation légale de ces outils, il est donc exclu que ceux-ci soient le moyen de réalisation de manquements aux obligations statutaires ou d’infractions de droit commun, l’utilisateur s’exposant dans ce cas à des sanctions disciplinaires et/ou des poursuites judiciaires.

Dans le cadre de cette responsabilité, et lorsque l’employeur détient des présomptions sérieuses d’infraction aux règles de la charte, il peut être amené à contrôler la légalité de l’utilisation de ces outils :

* une analyse du contenu des messages et fichiers professionnels,
* une analyse des connexions internet par les fichiers de « journaux » (dont la durée de conservation ne dépassera pas 3 mois),
* un blocage de l’accès à certains sites considérés comme dangereux ou interdits au regard de leur contenu présumé.

L’employeur met à disposition des utilisateurs les moyens techniques (informatique et communication) et humains (administrateurs) nécessaires au bon déroulement de leurs missions.

L’employeur assure donc la sécurité technique et le fonctionnement des moyens techniques, par les missions de ses administrateurs :

* assurer et maintenir la sécurité du système, notamment par l’installation du système d’exploitation des ordinateurs et des mises à jour nécessaires (mission exclusive des administrateurs).
* accompagner dans l’utilisation des moyens informatiques et de communication, notamment par la formation, l’assistance pour la résolution de problèmes techniques, et l’information des contraintes de service liées au maintien du bon fonctionnement des moyens informatiques et de communication (par exemple : interruption de service, maintenance…).
* intervenir sur les outils en cas de force majeure : ils peuvent avoir momentanément accès aux ressources informatiques indispensables à la poursuite de l’activité du service, si possible après avoir informé l’utilisateur, et à l’exclusion de l’accès à des répertoires, fichiers et messages clairement identifiés ou expressément signalés comme lieu de stockage de données privées.
* analyser les éléments sources de problèmes techniques : la prévention et la résolution de problèmes techniques autorisent les administrateurs à analyser un certain nombre d’éléments relatif aux logiciels, aux flux de trafic et aux volumes stockés et notamment :

- l’ensemble des fichiers journaux,

- les fichiers stockés (format, taille, date…),

- les ressources matérielles et logicielles,

- les connexions au réseau (identifiants, dates et heures de connexions…),

- les échanges via le réseau,

- les connexions internet (identifiants de connexion, volumes de données transférées, date et heures de connexion…),

- les messages stockés (fréquence, taille des fichiers transmis…).

Dans ce cadre, la confidentialité des données sera respectée (devoir de réserve et de secret professionnel des administrateurs).

L’employeur, informé par les administrateurs, prendra les mesures correctives et préventives nécessaires en cas de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal et de façon plus générale toute atteinte à la sécurité et manquement substantiel à cette charte.

## Données nominatives - RGPD

Des dispositions légales ont été prévues pour garantir les droits de toute personne en ce qui concerne le traitement de données nominatives la concernant. Dans ce contexte, la collectivité s’engage à respecter les dispositions de la loi informatique et libertés du 6 janvier 1978 modifiée et du règlement général sur la protection des données (RGPD).

Lorsque des données à caractère personnel sont collectées, cette personne est notamment informée :

* des finalités du traitement auquel sont destinées les données à caractère personnel, ainsi que de la base juridique du traitement,
* des destinataires ou des catégories de destinataires des données à caractère personnel, s’ils existent,
* de son droit d’accès permanent à ses données à caractère personnel,
* de la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée,
* de l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données selon le fondement du traitement,
* qu’aucune information concernant ses croyances, idéologies, appartenances politiques, mœurs sexuelles, appartenances raciales ou ethniques ne sera collectée.

Pour exercer ces droits, cette personne peut contacter le Délégué à la Protection des Données (DPD) de la collectivité : indiquer le nom et les coordonnées du DPD.

L’utilisateur traitant ces données à caractère personnel traitées dans l’exercice des fonctions s’engage à le faire de manière à assurer l’application de la réglementation sur la protection des données personnelles.

# DEPART D’UN UTILISATEUR

Lors de son départ, l’utilisateur doit restituer aux administrateurs l’ensemble des matériels mis à sa disposition, en état normal de fonctionnement, dont les fichiers et données personnelles auront été préalablement effacés.

Toute copie de documents professionnels doit être autorisée par le supérieur hiérarchique. Les comptes et les données personnelles de l’utilisateur sont, en tout état de cause, supprimés dans un délai d’un mois (jusqu’à 3 mois maximum) après son départ.

# SANCTIONS DE L’UTILISATEUR

L’utilisateur est responsable de l’usage qu’il fait des matériels informatiques mis à sa disposition.

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d’engager la responsabilité de l’utilisateur et d’entraîner des sanctions à son encontre.

Des sanctions en interne peuvent être prononcées, elles consistent :

* dans un premier temps, en un rappel à l’ordre émanant du Maire/Président/de la direction de la collectivité,
* dans un second temps, et en cas de renouvellement, après avis du Maire/Président/de la direction et du supérieur hiérarchique de l’utilisateur, en des sanctions disciplinaires.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d’information est susceptible de sanctions pénales et/ou civiles prévues par la loi.

# PRET DE MATERIELS

L’utilisateur doit renseigner et signer un registre, mis à disposition au service à préciser, actant la remise de l’équipement nomade ou encore la mise à disposition d’un matériel spécifique pour la tenue d’une réunion (vidéoprojecteur, ordinateur portable, appareil photo…).

Il en assure la garde et la responsabilité et doit informer le service à préciser en cas d’incident (perte, vol, dégradation) afin qu’il soit procédé aux démarches telles que la déclaration de vol ou de plainte.

Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements.

Le retour du matériel est également consigné dans le registre.

# RECEPISSE DE LA CHARTE D’UTILISATION DU SYSTEME D’INFORMATION

Je soussigné(e),

Nom :

Prénom :

Service :

Fonction : ,

reconnais avoir pris connaissance des dispositions de la charte d’utilisation des systèmes d’information de la collectivité qui m’a été notifiée.

Fait à .................................., le .........................

Signature