Charte informatique

PREAMBULE

L'usage des moyens numériques mis à disposition doit permettre de préserver le système d'information, le bon fonctionnement des services et les droits et libertés de chacun.

L'objectif de la présente charte informatique, document d'information et de référence, est donc de formaliser les règles légales et de sécurité relatives à l'utilisation de tous les outils d'information et de communication au sein de la collectivité.

Une mauvaise utilisation des différents outils technologiques utilisés peut entrainer des conséquences graves : risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité, risque d'atteinte à l'intégrité et à la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vols de données).

Chaque utilisateur doit avoir conscience qu'il joue un rôle actif dans ce contexte. Il s'engage à respecter la présente charte.

TABLES DES MATIERES

CHAMPS D'APPLICATION DE LA CHARTE

La présente charte s'applique à l'ensemble du personnel tous statuts confondus et aux utilisateurs du système d'information de l'Imprimerie Floch.

Elle s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques de la collectivité. Tout contrat avec un prestataire extérieur devra faire référence et comporter comme annexe la présente charte.

La charte annexée au règlement intérieur du personnel et s'impose de fait à chaque agent œuvrant au sein des services municipaux.

POSTES INFORMATIQUES

Tout utilisateur œuvrant dans/pour l'Imprimerie Floch peut disposer d'un droit d'accès au système d'information.

Ce droit d'accès est :

- ✓ **Strictement personnel**
- ✓ **Incessible**

Un ensemble « matériels - système d'exploitation – logiciels » est mis à disposition de chaque utilisateur, ce matériel est fragile, il convient d'en prendre soin et il est sous la responsabilité de l'utilisateur.

Pour les ordinateurs portables, il est important de ne pas les laisser à vue d'autrui et sans surveillance.

<u>Règles d'usage impératives</u> :

Les règles ci-dessous s'imposent à chaque utilisateur :

- En cas d'absence momentanée, l'utilisateur doit verrouiller son ordinateur (Astuce gain de temps : combinaison de touche Windows + « L »)
- A la fin de sa journée de travail, l'utilisateur doit fermer les applications et arrêter le système par arrêt logiciel (c'est à cette condition que les mises à jour essentielles sont installées), sauf poste définit.

Les supports extérieurs amovibles (clé USB, disque dur externe, etc.) personnels ou professionnels sont STRICTEMENT INTERDITS. Ils sont les premiers véhicules de virus.

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations. Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier du serveur n'est pas absolue et qu'il en reste une copie. Aussi, un utilisateur supprimant par erreur des données sur le serveur doit en informer immédiatement le service informatique afin que ce dernier puisse récupérer les données perdues. D'une manière générale, l'utilisateur doit signaler tous dysfonctionnements ou anomalies au service informatique.

ACCES WIFI

Les accès par le WIFI au réseau se fera via l'accès Floch_Public pour toute personne externe, l'accès Floch_Public ne donne pas l'accès aux données de l'Imprimerie Floch.

Pour tout autre matériel, l'accès est Floch_Prive ou Floch_Prive_Mdp, l'identification est soit par mot de passe ou certificat (Téléphone, tablette, portable PC/MAC, etc).

L'accès par un câble (RJ45) est interdit sauf pour les postes référencés.

GESTION DES IDENTIFIANTS ET MOT DE PASSE

Chaque utilisateur du réseau informatique se voit attribuer un compte auquel sont associés un identifiant (login) et un mot de passe. Il est responsable de l'utilisation qui est faite de ce compte et il lui appartient donc de ne pas communiquer son mot de passe à une tierce personne. À cet effet, il ne devra être noté sur aucun support et est, par sa nature, incessible et intransmissible.

Cas particulier : groupe d'utilisateur utilisant un même poste pour des usages ciblés.

Chaque mot de passe donnant accès à des données stratégiques (dont mot de passe donnant accès à la session) doit obligatoirement être modifié tous les 6 mois au minimum. Un mot de passe doit, pour être efficace, comporter au moins 15 caractères dont au moins une lettre en majuscule et une en minuscule et un numéro, Il ne doit pas, par ailleurs, reprendre le nom ou prénom de l'utilisateur ou le nom de l'entreprise.

Privilégier les phrases de mot de passe.

Le service informatique met à disposition un gestionnaire de mot de passe pour faciliter la gestion et le renouvellement des mots de passes.

MESSAGERIE ELECTRONIQUE

La messagerie est l'un des premiers vecteurs de propagation des virus et de « phishing » (technique utilisée par des escrocs pour collecter des données personnelles).

Il est en effet très simple de diffuser par courriel un fichier attaché contenant un virus ou un lien Internet pour inciter à télécharger un programme infecté.

Au même titre que pour le courrier papier ou le téléphone, chacun est responsable des messages envoyés ou reçus et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues et des règles élémentaires de courtoisie et de bienséance.

Un message envoyé par Internet peut potentiellement être intercepté, même illégalement, et lu par n'importe qui.

Utilisation privée de la messagerie :

L'utilisation de la messagerie est réservée à des fins professionnelles. Néanmoins il est toléré en dehors des heures de travail un usage modéré de celle-ci pour des besoins personnels et ponctuels.

Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'administrateur informatique (même en l'absence de l'utilisateur).

Ainsi, pour assurer la continuité du bon fonctionnement de l'entreprise, l'administrateur informatique, sur demande d'une autorité supérieure peut accéder à la messagerie d'un utilisateur absent en respectant la législation en vigueur et sous certaines conditions : il est notamment interdit à quiconque de prendre connaissance d'un message professionnel ayant pour objet « Personnel » ou « Confidentiel », sans l'autorisation expresse de l'utilisateur (qu'il en soit l'auteur ou le destinataire).

Règles d'usage :

- L'utilisateur veillera à ne pas ouvrir les mails dont le sujet paraîtrait suspect (pièces jointes, liens, ...)
- Une analyse des pièces jointes est effectuée en temps réel à l'ouverture d'un document envoyé par mail. L'antivirus va bloquer la pièce jointe en cas de suspicion de programme malveillant, mais attention, certains peuvent passer entre les mailles du filet.

Si vous recevez un mail que vous trouvez suspect, il est possible de l'envoyer à "bonjour@imprimeriefloch.fr" ou "hello@imprimeriefloch.fr"

- L'utilisateur s'engage à ne pas envoyer en dehors de l'entreprise des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel et autorisé par son supérieur hiérarchique.

- L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.
- L'utilisateur doit vérifier le contenu et l'historique des messages transférés.
- L'utilisateur doit éviter de surcharger le réseau d'informations inutiles. Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être nettoyé périodiquement.
- En cas d'absence, l'utilisateur devra mettre en place un message automatique indiquant la date de retour prévue et l'interlocuteur auquel s'adresser en son absence.

UTILISATION D'INTERNET :

L'utilisation d'Internet est réservée à des fins professionnelles dans le cadre de l'exercice des décharges d'activité. Néanmoins, il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise :

- De communiquer à des tiers des informations techniques concernant son matériel
- De diffuser des informations sur l'entreprise via des sites Internet

<u>Aussi l'utilisateur s'engage :</u>

- Lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine : 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.
- À ne pas télécharger, en tout ou partie, des données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.)
- À ne pas télécharger des logiciels, des vidéos, des photos n'ayant aucun lien avec les fonctions ou les activités professionnelles.

Pour éviter les abus, l'administrateur informatique peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes.

SIGNATURE ELECTRONIQUE ET CERTIFICAT :

Certains utilisateurs, dans le cadre de leurs fonctions, sont amenés à utiliser des certificats de signature électronique pour signer des documents et/ou s'authentifier pour accéder à des services sécurisés.

Ces certificats sont nominatifs et non cessibles, ils sont constitués de 3 éléments indissociables :

- Les informations concernant l'identité du titulaire, son organisation, sa fonction, la période de validité du certificat et l'identité de l'autorité de certification qui l'a généré,
- La clé privée
- La clé publique

L'utilisateur doit ainsi veiller à garder confidentiel le code à saisir (clé privée) lors de la signature avec son certificat. Les certificats ont une durée de validité limitée.

Toutes les demandes de certificat ou de renouvellement devront être validés par le service informatique.

Les certificats seront révoqués lorsque leur utilisateur quitte l'entreprise ou ne dispose plus de l'habilitation à l'utiliser.

PARE-FEU :

Le pare-feu vérifie tout le trafic de l'entreprise, aussi bien local que distant. Il détient toutes les traces de l'activité qui transite par lui s'agissant :

- De la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels)
- Des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe.

Il filtre notamment les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes.

TELEPHONIE OU TABLETTE

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 à condition que cela n'entrave pas l'activité professionnelle.

En cas d'absence, l'utilisateur doit :

- Ou effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique
- Ou laisser un message d'absence sur la messagerie téléphonique portable
- Ou verrouiller sa messagerie téléphonique sur son portable
- Le smartphone/tablette est un outil de travail dont l'usage personnel peut être autorisé (mention "personnel" pour messages personnels)
- Il n'est pas obligatoire de répondre aux appels ou aux mails en dehors du temps de travail (soir, weekend et congé sauf astreinte)
- Le smartphone/tablette ne doit pas venir perturber une réunion ou un entretien qui nécessitent la présence physique et intellectuelle de chacun.

DEPART D'UN UTILISATEUR

Tout utilisateur, lors de la cessation de son activité au sein de l'entreprise, perd son habilitation à utiliser les systèmes d'information internes. Il doit :

- Restituer tous les matériels mis à sa disposition
- Effacer de son poste de travail tous ses éventuels fichiers et données privés.

Il ne peut effectuer une copie de son travail professionnel qu'après autorisation écrite de son supérieur hiérarchique dûment habilité.

Les éventuels répertoires personnels ainsi que les données de messagerie des utilisateurs situés sur le serveur seront obligatoirement supprimés par l'administrateur informatique, en tout état de cause dans un délai maximum d'un mois après son départ.

MANQUEMENT A LA CHARTE

Le non-respect des règles édictées dans cette charte peut amener l'entreprise à suspendre, voire supprimer, l'accès des contrevenants à ces outils de communication.

En fonction de la gravité, des sanctions disciplinaires peuvent être prises selon la réglementation en vigueur et une procédure pénale peut être engagée.