# Charte Informatique de Formation

**Formation** met en œuvre un système d'information et de communication nécessaire à l'édition de livres et magazines. Elle met ainsi à disposition de ses collaborateurs des outils informatiques, et de communication. La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication de Microsoft. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle de Formation.

D'une manière générale, l'utilisateur doit s'imposer le respect des lois et, notamment, celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire, sur le harcèlement sexuel/moral.

**LE CHAMP D'APPLICATION DE LA CHARTE**
La présente charte s'applique à tout utilisateur du Système d'Information et de communication de **Formation** pour l'exercice de ses activités professionnelles. L'utilisation à titre privé de ces outils est interdite. La charte est diffusée à l'ensemble des utilisateurs par note de service et, à ce titre, mise à disposition sur l'intranet de l'entreprise. Elle est systématiquement remise à tout nouvel arrivant. Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

**Quelques définitions :**
On désignera sous le terme « utilisateur » toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de l'Entreprise et à les utiliser : employés, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels....
Les termes "outils informatiques et de communication" recouvrent tous les équipements informatiques, de télécommunications et de reprographie de Formation.

**OBLIGATIONS DES UTILISATEURS**
**1) Sécuriser l'accès au compte**

Le contrôle d'accès logique permet d'identifier toute personne utilisant un ordinateur. Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.bUne identification (login + mot de passe) unique est confiée à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas la communiquer.

Un mot de passe doit, pour être efficace, comporter au moins :

- 8 caractères alphanumériques répondant aux exigences de complexité (Ponctuation, Majuscule, minuscule, nombre.).
- Il ne doit pas être, notamment, identique au login, même en inversant les caractères, comporter le nom et/ou prénom de l'utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu,
- Etre écrit sur un document et être communiqué à un tiers.

**2) Courrier électronique**

Les éléments de fonctionnement de la messagerie à considérer sont les suivants :

- Un message envoyé par Internet peut potentiellement être intercepté, même illégalement, et lu par n'importe qui. En conséquence, aucune information stratégique ne doit circuler de cette manière, sauf sur autorisation du DSI.

- Il est interdit d'utiliser les services d'un site web spécialisé dans la messagerie. Nous n'utiliserons que la messagerie interne pour échanger des emails. Aucune connexion à sa boîte de messagerie personnel ne sera autorisée.

- Lors du départ d'un collaborateur, l'ensemble des fichiers et courriers électroniques de l'utilisateur qui ne sont pas de l'ordre privé seront analysés, le reste supprimé.

- Les messages électroniques sont conservés sur le serveur de messagerie pendant une période de 15 jours et il existe des copies de sauvegarde pendant une période de 30 jours.

- Ces copies de sauvegarde conservent tous les messages au moment où ils passent sur le serveur de messagerie, même s'ils ont été supprimés ensuite par leur destinataire.

**2.1 Utilisation privée de la messagerie**
L'utilisation du courrier électronique à des fins personnelles est interdites.

**2.2 Contrôle de l'usage**
Dans l'hypothèse la plus courante, le contrôle éventuellement mis en œuvre porte sur :
- Le nombre des messages échangés si supérieur à 30 sur une période d'une semaine ;
- La taille des messages échangés si supérieur à 20 mo. ;
- Le format des pièces jointes si epub, pdf, jpg, tout autre format d'image ou vidéo.

**3) Utilisation d'Internet**

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise :
- De communiquer à des tiers des informations techniques concernant son matériel ;
- De connecter un micro à internet via un modem *(sauf autorisation spécifique)* ;
- De diffuser des informations sur l'entreprise via des sites internet ;
- De participer à des forums *(même professionnels)* ;
- De participer à des conversations en ligne (« chat »).

**3.1 Utilisation d'Internet à des fins privées**
L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel et soient faites durant le temps de pause.

**3.2 Contrôles de l'usage**
Dans l'hypothèse la plus courante, les contrôles portent sur :
- Les durées des connexions supérieures à 2h par jour ;
- Les sites les plus visités

La politique et les modalités des contrôles font l'objet de discussions avec les représentants du personnel.

**4) Pare-feu**

Le pare-feu vérifie tout le trafic sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de fichier ou navigation sur internet.

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 et texte du message.
- Il filtre 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.

**5) Sauvegardes**

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations et un dispositif miroir destiné à doubler le système en cas de défaillance.

Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier de son disque dur n'est pas absolue et qu'il en reste une copie :

- Sur le dispositif de sauvegarde ou miroir ;
- Sur le serveur ;
- Sur le proxy ;
- Sur le firewall (pare-feu) ;
- Chez le fournisseur d'accès.

**ANNEXE**
**DISPOSITIONS LEGALES APPLICABLES**

Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004.
Dispositions Pénales :
- Code Pénal (partie législative) : art 226-16 à 226-24
- Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain. Dispositions pénales : art 323-1 à 323-3 du Code pénal.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

Règlement UE 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (RGPD)

Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels. Disposition pénale : art L.335-2 du Code pénal.

Fait à PARIS, le 28/05/2018

Signature de l'employeur