# ANNEXE

## Charte numérique de l'usager

### PRÉAMBULE

La charte concerne tous les usagers ou stagiaires autorisés à utiliser les ressources du système d'information de l'Afpa, ci-après dénommés **UTILISATEURS.** Elle est mise à disposition dans les lieux de mise à disposition des ressources. Annexée au règlement intérieur, elle précise les obligations des utilisateurs dans ses interactions avec le système d'information de l'Afpa.
Les utilisateurs sont tenus au respect des règles énoncées, dont le rôle est d'assurer la sécurité et la performance du système d'information, dans le respect de la législation et de la réglementation applicables.

#### 1 - PRINCIPES ESSENTIELS DE SÉCURITÉ

Chaque utilisateur est acteur de sa sécurité et doit y contribuer en prenant à son compte les termes de la charte.

Chaque utilisateur est responsable de son poste de travail et de ses moyens d'authentification. Sa responsabilité personnelle peut être engagée en cas d'acte de malveillance, d'action abusive ou d'action illicite réalisée sous son identité. Il est rappelé que chacun doit :

- protéger ses identifiants et mots de passe en les modifiant régulièrement et sans jamais les communiquer à un tiers ni les inscrire sur un support (papier, pense-bête ou autre),
- respecter les règles de complexité (nombre minimal de caractères alphanumériques, introduction de minuscules, majuscules, nombres et de caractères spéciaux),
- s'interdire d'utiliser l'identifiant et le mot de passe d'autrui,
- ne jamais quitter son poste de travail en laissant sa session ouverte,
- ne pas commettre d'action pouvant saturer la bande passante du réseau et affecter la disponibilité des systèmes d'information de l'Afpa (exemples : écoute de radio en ligne, visionnage de vidéo en streaming...).

Chacun doit respecter la législation en vigueur et notamment ne pas consulter, produire, copier, télécharger, diffuser des informations dont le contenu présente un caractère pédophile, négationniste, extrémiste ou portant atteinte à la dignité humaine.

Ces actes constituent une infraction au code pénal.
Il est interdit à un utilisateur d'user de ses codes d'accès pour accéder ou tenter d'accéder à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation d'accès.

En aucun cas l'utilisateur ne doit modifier les paramètres de sécurité établis par le service informatique sur les ressources du système d'information mises à sa disposition.

#### 2 - UTILISATION DES SYSTÈMES D'INFORMATION

**Utilisation professionnelle**

Compte tenu du risque d'introduire des virus ou des programmes malveillants dans le système d'information, l'utilisateur ne doit pas installer sur le réseau local ou sur sa machine des logiciels susceptibles de contourner ou d'affaiblir les dispositifs de sécurité du système d'Information de l'Afpa. En cas de nécessité, il ne peut le faire qu'avec l'autorisation expresse et écrite du manageur de formation ou du responsable de la salle.

**Utilisation privée résiduelle**

L'Afpa tolère l'utilisation à des fins privées des ressources du système d'information mises à disposition, dans la mesure où elle reste résiduelle tant dans la fréquence que dans la durée. Cette utilisation ne doit pas :

- affecter le bon fonctionnement du système d'Information,

• remettre en cause la sécurité de son poste et plus généralement celle du système d'Information.

L'Afpa respecte le caractère confidentiel de cette utilisation ponctuelle privée dès lors que cette dernière est signalée comme telle. Il appartient à l'utilisateur de nommer « personnel » le dossier dans lequel il stocke ses informations privées.

L'utilisateur veille à ne pas enregistrer ses identifiant et mot de passe personnel sur les postes de travail pour ne pas permettre une authentification automatique en son nom par un tiers.

**Utilisation d'Internet**

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources Internet mises à sa disposition. Seuls ont vocation à être consultés les sites Internet liés à la formation suivie, à la formation professionnelle en général et aux sites liés à l'emploi, sous réserve que la durée de consultation n'excède pas un délai raisonnable et présente une utilité au regard du profil de l'utilisateur.

La consultation d'un site pour motifs personnels dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs est tolérée à condition d'être opérée en dehors du temps de formation et d'être occasionnelle. Outre le respect de la réglementation rappelée dans le paragraphe « Principes essentiels de sécurité », l'utilisateur est tenu, notamment de :

• ne pas se connecter à des chaînes de radio ou de télévision ni de télécharger des fichiers musicaux, des films, des images ou des logiciels, qui génèrent de l'encombrement et un risque de violation de la propriété intellectuelle,

• ne pas participer au nom de l'Afpa à des forums, chats, blogs ou réseaux sociaux, et de ne pas porter atteinte à son image et à sa réputation,

• ne pas participer à des jeux de toute nature et/ou commettre tout agissement visant à obtenir des profits ou gains personnels.

Lors de l'utilisation de sa messagerie personnelle, l'utilisateur doit veiller à ne pas perturber le fonctionnement normal du réseau par l'envoi de messages de nature à augmenter les temps de réception et d'envoi (chaînes de solidarité, pièces jointes volumineuses…) sous réserve d'une durée d'utilisation raisonnable.

**Utilisation des matériels nomades**

L'utilisateur ne peut connecter de matériel nomade personnel au réseau de l'Afpa qu'après autorisation du manageur de formation. L'utilisation de supports de stockage personnels (clé USB, CD…) est prohibée, sauf en cas d'autorisation préalable du manageur de formation.

**Utilisation des accès distants**

Lorsqu'un accès à distance est accordé à un utilisateur, celui-ci s'engage à n'utiliser que les moyens d'authentification qui lui seront remis. L'utilisateur ne doit utiliser les moyens d'accès à distance qui lui sont fournis que dans le cadre de son activité à l'Afpa et conformément aux procédures et recommandations en vigueur à l'Afpa. Sont inclus tous les points de connexion spécifiques mis à disposition sur l'emprise de l'Afpa (ligne spécialisée, borne wifi…).

## 3 - DROITS DE PROPRIÉTÉ INTELLECTUELLE ET PROTECTION DES INFORMATIONS DE L'AFPA

En application de la législation relative à la propriété intellectuelle, les logiciels, supports, brochures, documents, cours, sujets et corrections d'examen ou tout autre document en général, mis à disposition de l'utilisateur pour les besoins de sa formation, sont propriétés de l'Afpa ou de ses donneurs de licence. L'utilisateur ne doit pas communiquer, sous quelque forme que ce soit (photocopie, photographie, document numérisé…), à des tiers non autorisés les produits cités au paragraphe ci-dessus. En conséquence, l'exploitation, la reproduction, le téléchargement, l'installation, l'adaptation, la traduction, la commercialisation et la représentation par tout procédé de communication de tout ou partie de ceux-ci sont interdites.

## 4 - MOYENS ET PROCÉDURES DE SÉCURITÉ

**Gestion des sorties de formation**

À la date de fin des prestations dues par l'Afpa à l'utilisateur, son répertoire estampillé « personnel » et stocké sur le réseau de l'Afpa est supprimé. Il appartient à l'utilisateur de récupérer et de supprimer ses fichiers avant la fin de sa formation.

**Surveillance et contrôle**

À des fins de sécurité et de vérification du bon accès et usage des ressources et dans les conditions légales applicables, l'Afpa se réserve le droit d'installer tous dispositifs permettant d'analyser, de limiter et de contrôler l'utilisation des ressources du système d'information ainsi que les échanges, effectués via le système d'information.

Ces contrôles seraient réalisés en considération du droit de l'utilisateur au respect de sa vie privée. S'agissant des messages personnels, peuvent faire l'objet de contrôles ayant pour but de protéger l'Afpa :

• des éléments tels que la fréquence et le volume des messages « personnel » qu'il émet et/ou reçoit,

• chaque connexion ou tentative de connexion, notamment la navigation sur Internet, l'usage de la messagerie électronique et l'accès aux applications et informations sensibles,
• les accès Internet, plus particulièrement les durées et les adresses IP de connexion, les adresses URL visitées, les demandes d'accès refusées par les mécanismes de filtrage de l'Afpa,
• l'usage des services de messagerie, plus particulièrement l'adresse mail des correspondants, les dates et heures d'envoi comme de réception, les textes des messages transmis et reçus, les pièces jointes,
• la connexion aux réseaux, applications et serveurs de fichier de l'Afpa, plus particulièrement les dates et heures de connexion, les références du poste connecté (adresse IP et autres éléments techniques d'identification de l'origine de la communication), les échecs de connexion, les opérations effectuées.

### 5 – SANCTIONS

Si toutefois l'utilisateur enfreint les règles définies dans cette charte, il est passible des sanctions disciplinaires prévues au règlement intérieur, sans préjudice d'éventuel recours à son encontre devant les juridictions compétentes à l'initiative de l'Afpa, du procureur de la République ou d'éventuels tiers victimes.

Dans le cas de tentative ou d'agissement frauduleux sur des sites distants accédés via Internet depuis le système d'information de l'Afpa, et si la responsabilité de l'Afpa était recherchée à côté de celle de l'utilisateur, l'Afpa se réserve expressément le droit d'appliquer à l'utilisateur les sanctions appropriées et d'exercer un recours contre lui.

Le manageur de formation pourra préciser certaines modalités d'application de la charte via des notes ou des affichages internes.

### 6 - QUE FAIRE EN CAS D'INCIDENT ?

L'utilisateur est tenu de signaler au manageur de formation, dans les plus brefs délais, tout incident de sécurité (apparition de virus, tentative d'intrusion ou intrusion) qu'il serait amené à observer.

L'utilisateur doit aviser sans délai le manageur de formation de la perte, du détournement ou du vol des moyens d'accès à distance et/ou d'authentification.

## GLOSSAIRE DE LA CHARTE NUMÉRIQUE

**Matériel nomade :** ressources du système d'information (ordinateur portable, smartphone, clé USB, carte de communication à distance…) qui sont appelées à être utilisées à l'extérieur de l'Afpa, en étant connecté ou non.

**Ressources du système d'information :** ensemble des moyens informatiques (ordinateur, PDA, smartphone…) et des supports (CD, DVD, clé USB…) légitimes qui sont mobilisés par les utilisateurs pour bénéficier du système d'information de l'Afpa.

**Utilisateur :** stagiaire ou usager qui bénéficie d'une formation Afpa ou de toute autre prestation Afpa, autorisé à accéder aux ressources du système d'information et au système d'information de l'Afpa.

**Système d'information :** système de traitement de l'information et de télécommunication de l'Afpa, qui fournit et distribue les informations et permet, *via* les ressources du système d'information, de les constituer, créer, échanger, diffuser, dupliquer, reproduire, stocker et détruire ; un système d'information inclut les services Internet.