



CHARTRE INFORMATIQUE DE **L'ASSOCIATION SAINT-FRANÇOIS** **D'ASSISE**

BONNE UTILISATION ET RESPECT DES OUTILS INFORMATIQUES

RAPPEL DES DROITS ET DEVOIRS DES UTILISATEURS

PROTECTION DES INFORMATIONS

Nombre de pages : 8

Association Saint-François d'Assise 60 rue Bertin CS 81010 97404 Saint-Denis Cedex – Site : www.asfa.re - Tél 0262 90 87 21 - Fax 0262 20 02 21 - E mail : directiongenerale@asfa.re

■ Hôpital d'Enfants 0262 90 87 00

■ Institut Médico-Educatif La Montagne 0262 23 63 64

■ Ecole de Puéricultrices 0262 90 87 77

■ EHPAD Saint-François 0262 90 87 69

■ PFS (SESSAD – SAMSAH) 0262 20 17 26

■ IFAP 0262 90 87 07

■ Résidence Retraite Médicalisée de Sainte-Clotilde 0262 93 96 00

■ Centre d'Education Motrice 0262 90 87 60

■ IRFE 0262 90 91 01

■ Centre d'Action Médico-Sociale Précoce 0262 90 87 87

■ MAS Franche Terre 0262 90 87 60

CHARTRE INFORMATIQUE ENTRE : L'Association Saint-François d'Assise

Représenté par M. Frédéric POTHIN

Ci-après dénommé « ASFA »

D'UNE PART

ET

Toute personne susceptible d'utiliser les outils informatiques proposés par l'ASFA

Ci-après dénommé « l'Utilisateur* »

D'AUTRE PART

*** L'utilisateur = salarié de l'ASFA et stagiaire (administratif et cycles supérieurs d'internat)**

1. Domaine d'application :

La charte définit les conditions générales d'utilisation de l'informatique à l'ASFA. Elle fixe les responsabilités de chacun, en accord avec la législation et permet ainsi de protéger l'ASFA et l'utilisateur.

Elle précise les droits et obligations que l'ASFA et l'Utilisateur s'engagent à respecter, et notamment les conditions et les limites des éventuels contrôles sur l'utilisation des services proposés.

Le non-respect des principes de cette charte pourra donner lieu à une limitation ou suppression de l'accès aux services, à des sanctions disciplinaires prévues dans le règlement intérieur ou pénales prévues par les lois en vigueur.

Cette charte a été validée par :

- le CA le : 23 juillet 2009

Soumise à l'avis de:

- la CME le : 31 mars 2010
- le CE le : 25 juin 2009
- le conseil de direction : 23 juin 2009

Ses mises à jour ont été validées par :

- le CA : le 18 décembre 2015

Soumise à l'avis de :

- la CME le : 2 février 2016
- le CE : le 26 août 2015
- le conseil de direction : le 10 septembre 2015

2. Respect de la législation :

a. La CNIL :

L'ASFA respecte les lois en vigueur en matière informatique et notamment celles érigées par la Commission Nationale de l'Informatique et des Libertés (CNIL). Un Correspondant (CIL) a été désigné, en la personne de la responsable informatique, qui s'occupe des déclarations, contrôle des affichages et rappel à la loi.

b. Internet :

La CNIL recommande un usage raisonnable de l'Internet au sein de l'Entreprise, non susceptible d'amoindrir les conditions d'accès professionnel au réseau, ne mettant pas en cause la productivité.

c. Les instances syndicales :

Aucun accord d'entreprise n'étant en vigueur, il est interdit aux représentants syndicaux d'utiliser l'Intranet de l'ASFA pour la diffusion de tracts et publications de nature syndicale.

d. Respect de la propriété intellectuelle :

Sont protégés par le droit de la propriété intellectuelle : logiciels, créations littéraires et artistiques, marques, dessins et modèles. Toute exploitation de ces éléments sans autorisation est une contrefaçon, qui constitue un délit. L'utilisateur ne doit pas procéder à une exploitation, reproduction, diffusion de ces éléments en dehors du cadre autorisé.

e. Informations :

Les informations contenant des données nominatives font l'objet d'une protection légale renforcée, et leur divulgation non autorisée peut faire l'objet de poursuites pénales.

f. Logiciels/licences :

L'ASFA détient des copies sous licence de logiciels informatiques publiés par différents éditeurs. Les copies enregistrées et sous licence de ces logiciels ont été installées sur les ordinateurs de l'association et les copies de sauvegarde autorisées ont été effectuées conformément aux accords de licence correspondants. Aucune autre copie des logiciels ou de leur documentation ne peut être effectuée sans l'autorisation écrite préalable expresse de l'éditeur.

g. Les administrateurs :

La CNIL a précisé dans une recommandation du 11 février 2002 que « tenus au secret professionnel, les administrateurs de réseaux et systèmes ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent pas en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. »

h. Droits de l'utilisateur :

L'utilisateur peut demander la communication des informations nominatives le concernant et les faire rectifier conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés.

i. Police des accès :

L'ASFA s'oblige à prévenir ou à faire cesser toute violation des droits d'un tiers en retirant les informations litigieuses accessibles par ses services ou en rendant l'accès impossible, dès lors qu'il en reçoit l'ordre par une autorité publique (Article 43-8 de la loi de 1986, modifié par la loi du 1^{er} août 2000).

j. Droit à l'image :

L'Utilisation de certains documents et images sont soumis à des règles (confidentialité, droit à l'image), l'utilisateur doit se rapprocher du service informatique avant de partager, diffuser des informations ou documents sur le réseau.

3. Domaine utilisation :

a. Applications dédiées aux informations patients :

Rappel de la loi et secret médical :

Loi du 4 mars 2002 relative à l'accès aux informations du dossier patient, en particulier l'article L1110-4

Secret professionnel :

Tout personnel ayant accès (via le logiciel métier ou non) à des informations sur les patients, est tenu au secret professionnel. Ces informations ne doivent être échangées que dans le cadre professionnel et dans le seul but de la prise en charge du patient.

Les utilisateurs d'applications métiers doivent y accéder qu'avec leurs seuls Login et mot de passe remis par les responsables des codes d'accès de ces applications (service informatique, DIM, cadre, cellule DPI...). Ces codes ne doivent servir qu'à consulter ou enregistrer des données dans le cadre professionnel, en lien avec la prise en charge du patient.

Toute action réalisée dans ces applications est tracée et archivée au nom de l'utilisateur concerné. Tout utilisateur est donc responsable des informations qui sont saisies ou consultées avec sa signature (Login), et ne doit donc en aucun cas donner ces codes d'accès à autrui.

b. Usage personnel :

L'usage personnel des moyens informatiques mis à la disposition des utilisateurs fait l'objet d'une tolérance. Cet usage doit rester modéré, ne pas avoir d'impact sur l'activité professionnelle du salarié et ne pas perturber ou influencer le fonctionnement du réseau informatique de l'ASFA. La direction informatique se réserve le droit d'interrompre l'accès à des services utilisés de façon non professionnelle ou dangereuse.

Les données personnelles, privées ne devront pas être stockées dans les répertoires de sauvegarde des ordinateurs. La direction se réserve le droit de les enlever. Ils devront être stockés dans un répertoire nommée **PRIVE**, situé hors réseau ASFA (sur le bureau ou support amovible par exemple).

c. Messagerie personnelle :

La consultation de sa messagerie personnelle via des outils professionnels est autorisée, mais doit être utilisée de façon modérée et n'entravant pas le bon déroulement des tâches professionnelles et du réseau de l'ASFA.

d. Messagerie professionnelle :

Quel que soit le type de messagerie, l'utilisateur ne doit pas utiliser les moyens de communication de façon susceptible de constituer un comportement illicite, ceci comprenant :

- la diffusion de rumeurs ou d'informations mal fondées,

- la diffusion de messages à caractère injurieux, pornographique, pédophile, raciste ou diffamatoire,
- tout comportement susceptible de porter atteinte aux intérêts de l'ASFA,
- une atteinte à l'intimité de la vie privée d'une personne
- l'utilisation ou la diffusion non autorisée d'éléments protégés par la propriété intellectuelle
- la réponse à des messages publicitaires

e. Consultation de site Web à titre personnel :

L'utilisateur s'engage à ne jamais consulter de site dont le contenu pourrait avoir un caractère raciste, antisémite, xénophobe, pornographique ou pédophile, ainsi que tout site relevant d'une activité illicite ou contraire à l'ordre public et aux bonnes mœurs.

f. Création de site Internet ou de pages Web :

L'utilisateur ne doit pas créer ni exploiter de site Internet personnel ou de page Web personnelle à partir de son poste de travail.

g. Forum de discussion personnel :

La participation à des forums de discussion à titre personnel est interdite.

h. Forum de discussion professionnel :

Dans le cadre de sa participation à des forums de discussion à titre professionnel, l'utilisateur s'engage à toujours observer une attitude de courtoisie envers ses correspondants, et une obligation de réserve et de loyauté à l'égard de l'ASFA.

i. Protection des mineurs :

Le personnel de l'ASFA se doit de protéger les mineurs en les préparant, en les conseillant, et en les assistant dans leur utilisation de l'Internet et des réseaux numériques.

j. Logiciels :

Seul le service informatique de l'ASFA peut fournir et installer les logiciels sur les postes de travail.

k. Sauvegarde :

Des répertoires de stockage (Mes Documents, partages, ...) sont mis à la disposition des utilisateurs sur des serveurs accessibles depuis le réseau. Ces répertoires font l'objet de sauvegardes journalières. L'utilisateur doit s'assurer qu'au moins un répertoire sur son poste de travail, permet une sauvegarde de ses données. Le service informatique ne saurait être responsable de données perdues alors que celles-ci ne se trouvaient pas dans le répertoire de sauvegarde.

Il est interdit de stocker des informations personnelles, musiques, fichiers audio, ... tout fichier susceptible d'alourdir inutilement les outils professionnels, dans ce répertoire de sauvegarde.

l. Contrôle :

A des fins statistiques ou d'inventaire, de qualité de service ou de sécurité, la direction informatique procède à des vérifications :

- trafic réseau, Internet, audit qualité,
- contrôle de l'utilisation des messageries,
- ...

Ces contrôles peuvent être effectués de façon globale et anonyme, mais aussi de façon individuelle.

m. Disponibilité du service :

Le service informatique s'efforce de maintenir accessible le service qu'il propose de manière permanente. Cependant cette même équipe peut interrompre l'accès, notamment pour des raisons de maintenance et de mise à niveau, ou d'autres raisons techniques, sans pour autant être responsable des conséquences de ces interruptions. Dans la mesure du possible l'équipe informatique tient informés les Utilisateurs de ces interruptions.

4. Sécurité :

L'utilisateur est responsable des moyens informatiques et réseau mis à sa disposition.

a. Sécurité physique :

L'utilisateur doit protéger son environnement de travail (bureau et session fermés en son absence, ...). Il est responsable de l'usage qu'il fait des outils informatiques et s'engage à ne pas apporter volontairement de perturbations à leur fonctionnement.

b. Les PC portables :

L'utilisateur devra être vigilant pendant ses déplacements avec son PC portable. Il est seul responsable du matériel mis à sa disposition et doit donc tout mettre en œuvre pour le protéger.

c. Sécurité logique :

L'utilisateur doit respecter les consignes liées à l'utilisation de son mot de passe, lequel doit être changé régulièrement. Sauf cas spécifiques de groupe d'utilisateurs, les droits d'accès sont personnels, et disparaissent avec le départ du salarié.

Sauf autorisation de son supérieur hiérarchique, un utilisateur ne peut pas utiliser un autre compte que le sien.

Sauf autorisation de sa hiérarchie ou de la direction informatique, un utilisateur ne doit pas modifier le paramétrage des systèmes, utiliser des dispositifs logiciel ou matériels non autorisés.

L'utilisateur ne doit pas télécharger depuis Internet des fichiers ou programmes à l'origine non contrôlée et les installer sur les systèmes de l'ASFA

L'utilisateur ne doit se livrer à aucun test d'intrusion ou de sécurité sur le réseau de l'ASFA.

L'utilisateur doit signaler toute anomalie de fonctionnement à laquelle il aurait été confronté, par le biais de l'outil « GLPI ». Voir les procédures en cours de validité.

d. Antivirus :

Le réseau de l'ASFA est protégé par un antivirus d'entreprise mis à jour régulièrement sur les postes de travail connectés au réseau. Il est tout de même conseillé aux utilisateurs d'être extrêmement vigilants face aux virus, qui peuvent se propager de diverses façons (Sites Internet, messagerie, clés USB, ...). Les impacts peuvent être graves, la direction informatique sera donc très exigeante quant à l'utilisation à risque de l'outil informatique.

Il est également conseillé à l'utilisateur de s'inquiéter de la mise à jour de son antivirus et de se faire assister du service informatique pour s'assurer des mises à jour.

La direction se réserve le droit de limiter l'utilisation de tout support susceptible de nuire à la sécurité du réseau, comme les clés USB ramenant des virus.

e. Surveillance des activités :

Il incombe aux équipes pédagogiques de contrôler les activités liées à l'utilisation des outils informatiques par des élèves ou étudiants, et ce afin de pouvoir intervenir rapidement en cas de problème, à repérer et faire cesser tout comportement pouvant devenir dangereux.

f. Les procédures :

Il incombe au salarié de se tenir informé des procédures validées par la direction de l'établissement et en vigueur dans cet établissement et/ou au siège.

g. Le Wi-Fi :

Les accès au WIFI sont gérés par des référents en charge de délivrer des tickets d'accès. Une charte WIFI est en vigueur au sein de l'ASFA et signée par l'utilisateur lors de sa connexion au WIFI.

h. Les téléchargements :

Les téléchargements en libre accès (musique, photos, vidéos, ...) sont autorisés dans le cadre de l'activité professionnelle de l'utilisateur et non pour des raisons personnelles.

5. Protection des informations :

Le système d'information de l'ASFA comprend un certain nombre d'informations qui ne sont pas accessibles au public. Ces informations sont strictement confidentielles et ne doivent pas être transférées à l'extérieur de l'ASFA, que ce soit par le réseau Internet ou via un média quelconque. L'utilisateur veillera à ce que ses courriers électroniques ne comprennent que des informations pouvant être portées à la connaissance des destinataires du courrier, compte tenu des règles de confidentialité applicables.

a. Les administrateurs informatiques :

Dans l'exercice de leurs fonctions, les administrateurs informatiques peuvent avoir accès aux mots de passe des utilisateurs et aux informations qui transitent sur les postes de travail, les médias amovibles et les serveurs.

Les administrateurs sont tenus au secret professionnel. Ils s'engagent à n'utiliser les données à caractère personnel concernant l'utilisateur que pour les strictes finalités pour lesquelles elles ont été collectées.

Dans le cas où l'administrateur système saisi par une autorité judiciaire ou policière, en vue de lui communiquer des données relatives à un utilisateur, l'administrateur est habilité à communiquer les informations demandées dès lors que l'autorité judiciaire ou policière dispose des autorisations requises par la loi pour exercer cette demande.

Dans le cas où l'administrateur système serait saisi par un membre autorisé de la hiérarchie de l'ASFA en vue de lui communiquer des données relatives à l'utilisation des moyens informatiques et réseau de l'ASFA par un utilisateur, l'administrateur est habilité à ne pas communiquer les informations demandées dès lors :

- qu'elles ne contreviennent pas à la présente charte,
- et qu'elles ont un caractère personnel et confidentiel sans rapport avec l'activité professionnelle du salarié, ou qu'elles relèvent de l'exercice du droit d'expression des salariés, prévu à l'article L.461-1 du code du travail, et plus généralement de leur liberté d'expression.

b. Droits d'accès :

L'utilisateur ne doit pas essayer d'utiliser des droits autres que les siens, de masquer sa véritable identité ou d'usurper celle d'autrui.

Il ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent, directement ou indirectement.

Il ne doit pas se connecter ou essayer de se connecter sur un serveur, interne ou externe, autrement que par les dispositions prévues par ce serveur ou sans y être autorisé.

Il ne doit pas déposer des documents sur un serveur, sauf si celui-ci le permet, ou sans y être autorisé.