Charte de bon usage
des nouvelles technologies de l'information et de la communication
(ressources informatiques, services Internet, télécommunications)
à l' I.F.S.I/.I.F.A.S du Centre Hospitalier de CHAUNY[1]

Cette charte vaut pour règlement intérieur en ce qui concerne les nouvelles technologies de l'information et de la communication.

INTRODUCTION

Tout utilisateur est amené à utiliser les ordinateurs mis à sa disposition au sein de l'institut de formation. L'accès à ce matériel se fait sous la responsabilité de la directrice de l'établissement.

Tous les utilisateurs s'engagent à respecter :
• Les règles d'utilisation du matériel informatique définies au sein de l'Institut.
• La législation en vigueur.

Cette charte définit ces règles de bonne utilisation. Elle informe les divers utilisateurs des sanctions encourues en cas de non observation, en accord avec la législation en vigueur (voir Annexe).

I. QUELQUES DEFINITIONS

I.1 DESCRIPTION DES RESSOURCES INFORMATIQUES MISES A DISPOSITION

Les ressources informatiques de l'établissement sont constituées de serveurs, micro-ordinateurs, d'une classe mobile dotée de 17 ordinateurs portables, de 2 imprimantes, de logiciels, de données appartenant ou utilisés à l'IFSI/IFAS du Centre Hospitalier de CHAUNY et de réseaux interne et externe (Internet).

I.2 DEFINITION DE L'ADMINISTRATEUR SYSTEME D'INFORMATION ET ORGANISATION

Un administrateur système d'information et organisation est une personne physique ayant la responsabilité des ressources informatiques. Au Centre Hospitalier de CHAUNY cette fonction est assurée par le Responsable Système d'Information et Organisation.

I.3 DEFINITION DES UTILISATEURS

Un utilisateur est une personne autorisée par l'administrateur à accéder à l'une des ressources informatiques de l'établissement.

II. DROITS ET DEVOIRS DES UTILISATEURS

II.1 IDENTIFICATION DE L'UTILISATEUR

[1] Lire partout Institut de Formation en Soins Infirmiers/ Institut de Formation Aide-Soignante

Chaque utilisateur se voit attribuer un compte accessible par un mot de passe personnel. L'institut fournit à l'administrateur les données utiles à la création de ce compte (nom, prénom, date de naissance) et s'engage à l'informer en cas de reprise, d'intégration ou d'interruption de la formation.

II.2 CONDITIONS D'ACCES AUX RESSOURCES INFORMATIQUES ET SERVICES INTERNET

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques de l'établissement.

Le droit d'accès à une ressource informatique est personnel, incessible et peut être temporaire. Il est soumis à l'autorisation de l'administrateur et assorti de moyens d'identification. Il peut être retiré si les conditions d'accès ne sont plus respectées ou si le comportement de l'utilisateur est contraire à la Charte.

Les moyens d'accès ou d'identification (code, mot de passe) sont remis à titre personnel et sont incessibles. Ils ne peuvent être prêtés, donnés ou vendus à des tiers et sont rendus en fin d'activité.

L'utilisateur doit prévenir l'administrateur de tout accès frauduleux ou tentative d'accès aux ressources qu'il utilise. Il est responsable de la protection de ses fichiers et de l'accès à ses données.

II.3 RESPECT DU CARACTERE CONFIDENTIEL DES INFORMATIONS

Les fichiers possédés par un utilisateur sont considérés comme privés, qu'ils soient ou non accessibles à d'autres utilisateurs. La lecture, la copie ou la modification d'un fichier ne peuvent être réalisées qu'après accord explicite et par écrit de son propriétaire.

Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi "Informatique et Libertés" (Fichiers nominatifs), il devra auparavant demander l'autorisation à l'administrateur qui se doit d'accomplir les formalités légales auprès de la CNIL.

II.4 RESPECT MUTUEL DES PERSONNES

Un utilisateur ne doit ni porter atteinte à la vie privée et à la personnalité de quiconque ni nuire à l'activité professionnelle d'un tiers par l'utilisation de moyens informatiques.

II.5 RESPECT DE L'INTEGRITE DES RESSOURCES INFORMATIQUES

Le développement, l'installation ou la simple copie d'un programme par un utilisateur est interdite.

II.6 USAGE DES SERVICES INTERNET (WEB, MESSAGERIE, FORUM…)

L'interconnectivité permet une grande convivialité dans l'utilisation des ressources mondiales (Internet). C'est pourquoi l'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités au sein de l'établissement et dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

En particulier :

- Ne pas utiliser ces services pour proposer ou rendre accessibles aux tiers des données et informations confidentielles ou contraires à la législation en vigueur,
- Faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions,

- S'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire ainsi que celles qui véhiculent des idéologies (à caractère politique ou religieux) contraires aux grands principes fondamentaux de la république.

Toutes les connexions aux sites Internet sont enregistrées sur le serveur de l'établissement, l'administrateur est tenu de vérifier que la consultation d'un site est en adéquation avec le cadre de l'activité de l'utilisateur. A défaut il pourra lui interdire l'accès aux services Internet.

II.7 REGLES D'UTILISATION, DE SECURITE ET DE BON USAGE

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale.

- Tout compte utilisateur doit être protégé par un mot de passe.
- Un mot de passe ne doit pas être affiché même si le poste de travail est partagé par plusieurs personnes travaillant sur le même bureau.
- Un mot de passe ne doit jamais être donné à un tiers et un compte ne doit jamais être prêté.
- Des supports numériques (Disques durs externes, CD rom et clés USB) ne doivent jamais être abandonnés dans un bureau ouvert.
- L'utilisateur s'assure préalablement que les supports numériques qu'il utilise sont exempts de virus au risque de porter atteinte à l'intégrité du matériel de l'institut et des autres utilisateurs.
- Toute session de travail doit être terminée conformément à la technique d'utilisation requise. En cas d'incident ou de fin anormale, l'administrateur doit être prévenu immédiatement.
- Un poste de travail ne doit jamais être quitté lorsqu'une session est en cours.

Toute modification de paramétrage ne peut être effectuée que par l'administrateur ou par un technicien informatique.

III. DROITS ET DEVOIRS DE L'ADMINISTRATEUR

III.1 OUVERTURE DE COMPTE

L'administrateur ouvre des comptes aux utilisateurs ayant pris connaissance et signé le présent document. Il peut les fermer s'il a des raisons de penser que l'utilisateur transgresse les règles contenues dans la présente charte.

III.2 DISPONIBILITE DES RESSOURCES INFORMATIQUES

L'administrateur ou les techniciens informatiques doivent informer les utilisateurs des diverses contraintes d'exploitation (interruption de service, maintenance, modification des ressources,...).

III.3 RESPECT DE LA CONFIDENTIALITE

L'administrateur ou les techniciens informatiques doivent respecter la confidentialité des données des utilisateurs auxquelles ils peuvent être amenés à accéder.

III.4 ACCES AUX DONNEES PRIVEES ET CONTROLE DE L'UTILISATION DES RESSOURCES

L'administrateur ou les techniciens informatiques peuvent accéder à des données pour diagnostiquer ou corriger des problèmes spécifiques. Il est tenu à l'obligation de confidentialité.

Ils peuvent aussi, dans les mêmes conditions et s'ils l'estiment nécessaire, examiner les données et les communications des utilisateurs pour la bonne marche du système ou pour vérifier le respect de la Charte.

Ils peuvent modifier les conditions d'utilisation d'une ressource informatique afin d'en optimiser le fonctionnement ou de maintenir le bon état de cette ressource.

IV. SANCTIONS EVENTUELLES (VOIR ANNEXE)

IV.1 NOTION DE DELITS INFORMATIQUES (VOIR ANNEXE)

Les délits informatiques sont principalement de plusieurs types :

- Intrusion sur un ordinateur ou sur un réseau
- Réalisation, utilisation, installation ou diffusion d'une copie illicite de logiciels
- Vol de fichiers informatiques
- Divulgation d'informations
- Emprunt de l'identité d'un tiers.

IV.2 EXISTENCE D'UN DROIT DE L'INFORMATIQUE (SANCTIONS)

Il est rappelé qu'en plus des poursuites administratives, des poursuites judiciaires peuvent être engagées par la Direction de l'IFSI/IFAS du Centre Hospitalier de CHAUNY ou par toute victime, tant sur le plan pénal qu'en réparation du préjudice subi.

IV.3 SANCTIONS INTERNES

La tentative d'accès illicite à une ressource informatique de la part d'un utilisateur peut entraîner la suppression de tout accès à l'une ou l'autre des ressources informatiques de l'établissement.

Le droit d'accès peut être refusé à tout apprenant ayant contrevenu à la Charte. Les fautes peuvent être sanctionnées disciplinairement dans le cadre des peines prévues par le statut particulier de l'utilisateur.

Les utilisateurs ne respectant pas les règles et obligations définies dans cette charte sont passibles de sanctions internes à l'établissement.

IV.4 SANCTIONS PENALES

La direction de l'IFSI/IFAS du Centre Hospitalier de CHAUNY est tenue par la loi de signaler auprès des Tribunaux judiciaires toute violation des lois dûment constatée.

Toute personne ayant connaissance d'un délit relatif à l'informatique est tenue de le dénoncer dans les formes prévues par le Code de Procédure Pénale. (L'annexe de la présente charte contient, à titre d'exemples, les délits et peines les plus fréquemment rencontrés).

Tout utilisateur n'ayant pas respecté la législation pourra être poursuivi pénalement.

IV.5 SANCTIONS CIVILES

Les auteurs d'agissement contraires à la loi peuvent être condamnés à des réparations en dommages-intérêts aux victimes ayant subi des préjudices.

V. APPLICATION DE LA CHARTE

La présente charte s'applique à l'ensemble des élèves aides-soignants, des étudiants en soins infirmiers et des formateurs de l'établissement.

Un exemplaire de la Charte est remis à chaque apprenant à son entrée. La déclaration sur l'honneur annexée à celle-ci signée par l'utilisateur sera versée au dossier administratif de l'apprenant.

Annexe

Rappel des principales lois françaises

- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1).
- Loi n°85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle,
- Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique,
- Loi 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne en son article 29
- Code pénal et notamment les articles L323-1 à L323-7, L222-18-1, L226-1 à L226-8, L226-15 à L226-24, L227-23, L227-24 et L434-23
- Article 9 du code civil

Modifié par Loi n°94-653 du 29 juillet 1994 - art. 1 () JORF 30 juillet 1994
Modifié par Loi n°70-643 du 17 juillet 1970 - art. 22 () JORF 19 juillet 1970
Création Loi 1803-03-08 promulguée le 18 mars 1803

- Code de la propriété intellectuelle et notamment son article L122-6-1

Modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 25

- Le règlement général sur la protection des données - RGPD

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)

- Article 432-9 du Code pénal

Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 121 () JORF 10 juillet 2004

- Code de la Propriété Intellectuelle, loi du 10 mai 1994

L'article 335-2 interdit à l'utilisateur de logiciel toute reproduction autre que celle d'une copie de sauvegarde. Toute autre copie est considérée comme une contrefaçon et constitue un délit.
Sanctions prévues : jusqu'à 3 ans d'emprisonnement et 300 000 € d'amende.