

Charte pour l'utilisation des ressources informatiques à l'IUFM Orléans-Tours

1. Domaine d'application de la charte

Les obligations décrites dans la présente charte s'appliquent à toute personne (en particulier étudiant, stagiaire, enseignant, formateur, chercheur, personnel administratif ou technique) qui utilise les moyens informatiques de l'Institut et qui accède, à tout service de communication ou de traitement électronique interne ou externe, y compris l'accès aux services ouverts sur l'Internet.

2. Conditions d'accès de l'utilisateur

Chaque utilisateur reçoit en contrepartie de la signature de la présente Charte un droit d'accès individuel, en fonction de son activité (accès Internet, accès aux applications de gestion, accès à un compte courrier électronique ...)

Ce droit d'accès se matérialise, le cas échéant, par tout moyen logique ou physique (code d'accès, nom d'utilisateur, mot de passe, badge ...)

Dans le cas où l'utilisateur choisit un mot de passe, il doit le choisir sûr (d'au moins 8 caractères, ne figurant dans aucune langue), le garder secret et ne le communiquer en aucun cas à un tiers.

Ce droit d'accès est strictement personnel et incessible. Il cesse automatiquement lorsque l'utilisateur quitte l'Institut ou s'il est constaté qu'il a violé l'une des obligations imposées par la présente charte.

Le droit d'accès n'est conféré à l'utilisateur qu'aux fins d'une utilisation compatible avec les activités de l'Institut - qu'elles soient administratives, pédagogiques ou de recherche - et exclut toute autre utilisation, notamment commerciale.

L'utilisateur reconnaît que l'usage de son droit d'accès peut engager sa responsabilité dans les conditions précisées dans la présente charte.

Il est interdit à un utilisateur d'user de son droit d'accès pour 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. De même, il est interdit à tout utilisateur d'user, par quelque moyen que ce soit, du droit d'accès d'un autre utilisateur.

Les utilisateurs ne respectant pas les règles et obligations ci-dessus relèvent de la section disciplinaire du conseil d'Administration de l'IUFM qui exerce, en premier ressort, le pouvoir disciplinaire à l'encontre des contrevenants.

De plus, toute violation des conditions d'accès décrites ci-dessus peut entraîner, l'engagement de la responsabilité civile de son auteur et constituer une infraction réprimée par les articles 323-1 à 323-7 du code pénal.

3 Obligations de confidentialité

Chaque utilisateur ne peut accéder qu'aux informations ou fichiers mis publiquement à disposition sur le réseau, ainsi qu'à ses informations ou fichiers personnels. Il lui est interdit de chercher à prendre connaissance d'informations ou de fichiers réservés à l'usage d'autres utilisateurs, même dans le cas où ces éléments ne seraient pas protégés par des dispositifs physiques ou logiques. Toute violation de la présente obligation est susceptible d'engager la responsabilité civile ou pénale de son auteur.

4. Obligations relatives à la propriété des logiciels et des œuvres protégées par le droit d'auteur

Aucun utilisateur n'est autorisé à effectuer la copie des logiciels disponibles sur le réseau, même à des fins de constitution de copies de sauvegarde, qui ne peuvent être effectuées que par des personnes spécialement habilitées par l'Institut.

En dehors des logiciels, chaque utilisateur ne peut effectuer de copie d'œuvres protégées par le droit d'auteur que pour autant que celles-ci soient accessibles sans restriction d'usage sur le réseau et que la copie qu'il en effectue n'est destinée qu'à son usage strictement privé.

Toute violation de la présente obligation peut engager la responsabilité civile de son auteur et constitue une contrefaçon sanctionnée pénalement par les articles L.335-2 et suivants du Code de la propriété intellectuelle.

5. Installation de logiciels

Dans les cas des postes des services administratifs, l'utilisateur demande l'avis du SCIRC (Service Commun Informatique et des Réseaux de Communication) avant toute installation ou mise à jour d'un logiciel.

Dans le cas de postes servant à la formation, aucune personne en formation n'est autorisée à installer un logiciel (quel qu'en soit le type) sans l'accord du formateur.

A l'issue de la formation, le formateur s'engage à restituer la salle dans l'état de fonctionnement dans lequel il l'a trouvée en arrivant. Il pourra procéder à la restauration d'une image disque préalablement sauvegardée ou procédera à la désinstallation des logiciels qu'il aurait été amené à installer.

Concernant les postes des salles libre-service, ceux-ci doivent être utilisés sans tenter de modifier le paramétrage base de la machine ; en particulier l'installation par un usager de tout logiciel, quel qu'en soit le type, est interdite.

6. Obligations relatives aux données nominatives

Toute constitution, à l'aide des moyens informatiques de l'Institut, de données nominatives doit faire l'objet, sous la seule responsabilité de l'utilisateur, des déclarations ou des demandes d'avis prévues par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et doit respecter les obligations fixées par cette loi.

7. Obligations relatives aux moyens de cryptologie

L'utilisateur ne peut utiliser sur le réseau de l'Institut des moyens de cryptologie qui n'auraient pas fait l'objet au préalable des déclarations ou des autorisations imposées par l'article 28, modifié de la loi du 26 décembre 1990, portant réglementation des télécommunications.

8. Production et diffusion d'informations sur le réseau

Mis à part l'usage du courrier électronique à des fins de correspondance privée, aucune diffusion publique d'une information ou d'une œuvre ne pourra être effectuée sur le réseau informatique de l'Institut - sauf dérogation particulière accordée, à des fins pédagogiques ou de recherche par un responsable éditorial désignée par les autorités compétentes de l'Institut pour gérer la production d'informations sur le réseau.

9. Obligations relatives à la sécurité et à l'intégrité du système et des données

L'utilisateur reconnaît avoir pris connaissance des règles de sécurité liées à l'usage du réseau RENATER, auquel le réseau de l'Institut est connecté et s'engage à en respecter les obligations.

L'utilisateur s'engage à n'apporter - directement ou indirectement - aucune perturbation au fonctionnement du réseau et des systèmes informatiques auxquels il accède et à ne provoquer aucune modification, altération ou destruction concernant des données ou fichiers autres que ceux dont il est l'auteur.

L'utilisateur s'engage formellement à ne pas masquer sa véritable identité ou tenter d'usurper celle d'un autre utilisateur.

L'utilisateur s'engage formellement à ne pas procéder à des manipulations anormales du réseau, à ne pas introduire volontairement de logiciels parasites (virus, ver, Chevaux de Troie, logiciel d'écoute réseau...), à ne pas développer de tels outils en utilisant les ressources de l'Institut, à ne pas tenter de diminuer l'efficacité des mesures de protection mises en place.

Toute violation de ces obligations peut engager la responsabilité civile de son auteur et constituer une infraction réprimée par les articles 323-1 à 323-7 du code pénal.

L'utilisateur s'engage à signaler sans délai au SCIRC toute anomalie ou incident concernant la sécurité qu'il serait amené à constater.

10. Règles d'accès aux locaux et aux systèmes informatiques

Tout utilisateur accepte de se plier aux contraintes particulières définies par les différents services de l'IUFM pour l'accès à leurs locaux et à leurs moyens informatiques.

L'accès aux postes informatiques de l'Institut est strictement réservé aux formés, formateurs et personnels de l'Institut.

11. Contrôle de l'utilisation des ressources

Pour des nécessités de sécurité et de maintenance, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau sont contrôlés dans le respect de la législation applicable, par les R.S.S.I. (Responsables de la Sécurité des Systèmes d'information).

Les échanges effectués sur le réseau sont enregistrés dans des fichiers de traces. Dans le cas de la messagerie sont mentionnés en particulier l'expéditeur, le destinataire, la taille du message ; concernant l'accès Internet sont enregistrés notamment l'adresse du poste, les sites consultés, les fichiers téléchargés.

Ces fichiers de traces, analysés régulièrement, ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'une procédure judiciaire et après accord du Directeur de l'Institut ces fichiers peuvent être mis à la disposition de la justice.

12. Règles particulières concernant la messagerie électronique

La messagerie électronique est un service mis à la disposition des usagers de l'IUFM.

Cependant :

- l'utilisateur veille à appliquer les dispositions concernant le mot de passe détaillées au paragraphe 2
- l'utilisateur veille à supprimer les messages qui ne lui sont plus utiles dans le cas où ces messages sont conservés sur le serveur de l'Institut
- l'utilisateur n'envoie pas de messages de taille exagérée et ne procède pas à des envois massifs de courrier
- l'utilisateur limite l'envoi de pièces jointes et reste vigilant s'il est amené à en recevoir, celles-ci étant un vecteur privilégié de propagation des virus
- A l'examen du non respect des règles ci-dessus énoncées, le Directeur peut procéder à la fermeture du compte courrier électronique concerné.

13. Règles particulières concernant l'accès à l'Internet

Il est rappelé que l'accès Internet est offert aux usagers de l'IUFM à des fins strictement professionnelles, dans le cadre des activités techniques, administratives, d'enseignement, de recherche ou de formation liées à leur statut à l'IUFM.

L'attention de l'utilisateur est attirée sur le fait que l'utilisation des ressources informatiques de l'Institut à des fins autres que celles définies ci-dessus sera considérée comme une faute professionnelle ; en outre, si les sites consultés présentent un contenu illégal, l'Institut se verra contraint de porter plainte contre l'utilisateur concerné.

Il est rappelé d'autre part aux utilisateurs que le téléchargement de logiciels présente des risques importants et qu'il n'est donc pas autorisé sans l'avis du correspondant informatique ou du responsable de la formation concernée.

14. Responsabilités des parties

Chaque utilisateur accède et utilise les moyens informatiques et le réseau auquel il a accès sous sa propre responsabilité. Il reconnaît que toute violation des dispositions de la présente charte, ainsi que, plus généralement, tout dommage créé à l'Institut ou à des tiers de son fait engagera sa responsabilité, tant sur le plan disciplinaire, que civil ou pénal.

L'IUFM déclare mettre en œuvre - par le biais de la présente charte et des diverses mesures de sécurité physique et logique qui sont les siennes - tous les efforts nécessaires à un bon usage de ses systèmes et du réseau et n'assumer aucune responsabilité au titre des agissements fautifs ou délictueux des utilisateurs auxquels elle fournit un droit d'accès.