

CHARTRE DU BON USAGE DES RESSOURCES INFORMATIQUES DE L'UNIVERSITE LILLE 2

(approuvée par le Conseil d'administration du 30 juin 2005)

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques au sein de l'Université Lille 2. Elle a également pour objet de rappeler et préciser les responsabilités des utilisateurs dans le cadre de la législation en vigueur et la charte de déontologie RENATER afin de permettre un usage normal et optimal des ressources informatiques et des services Internet employés au sein de l'Université.

La présente charte constitue la partie « informatique » du règlement intérieur de l'Université. Elle sera régulièrement actualisée afin de tenir compte des évolutions juridiques et technologiques.

1. Champ d'application de la charte

Les règles et obligations énoncées par la présente charte s'appliquent à tout utilisateur . Est entendu comme utilisateur soumis à la présente charte : toute personne : enseignants, chercheurs, enseignants-chercheurs, étudiants, personnels administratifs ou techniques, personnels temporaires, stagiaires, etc ... ; utilisant les moyens et systèmes informatiques de l'Université de Lille 2.

Ces derniers comprennent notamment le réseau, les serveurs, stations de travail et micro-ordinateurs, y compris l'informatique nomade.

2. Conditions d'accès aux réseaux informatiques de l'Université

L'utilisation des moyens informatiques de l'Université a pour objet exclusif de mener des activités de recherche, d'enseignement ou d'administration. Sauf autorisation préalable délivrée par l'Université, ces moyens ne peuvent être employés en vue d'une utilisation ou de la réalisation de projets ne relevant pas des missions de l'Université ou des missions confiées aux utilisateurs dans le cadre de leur activité professionnelle ou pédagogique.

L'utilisation des ressources informatiques et la connexion d'un équipement sur le réseau sont soumis à autorisation. Le droit d'accès est toujours personnel, incessible et peut être temporaire.

Chaque utilisateur se voit attribuer des codes d'accès en fonction de ses besoins (accès internet, accès aux applications de gestion, accès à des serveurs particuliers, accès aux ressources documentaires, accès au campus virtuel, etc.). Les codes d'accès attribués sont strictement personnels et incessibles. **Chaque utilisateur est responsable de l'utilisation qui en est faite. Le mot de passe est fourni par le service informatique concerné. Chaque utilisateur s'engage à ne pas communiquer ce mot de passe à une tierce personne. Chaque utilisateur est personnellement responsable de son code d'accès et de son mot de passe.**

L'utilisateur avertira le correspondant informatique de sa composante si un code d'accès ne lui permet plus de se connecter, s'il soupçonne que son compte a été usurpé. D'une façon plus générale, il informera le correspondant informatique de sa composante de toute anomalie qu'il pourrait constater.

3. Respect des règles de la déontologie Informatique

Chaque utilisateur s'engage à respecter les règles de la déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- de masquer sa véritable identité ;
- de s'approprier le mot de passe d'un autre utilisateur ;
- d'altérer, de modifier des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau ou à l'Université, sans leur autorisation ;
- de porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par

- l'intermédiaire de messages, textes ou images provocants ;
- d'interrompre ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau ;
- de modifier ou de détruire des informations sur un des systèmes ;
- de se connecter ou d'essayer de se connecter sur un site sans y être autorisé.

La réalisation d'un programme informatique ayant de tels objectifs est également interdite.

Il est par ailleurs rappelé que tout utilisateur, se doit de respecter la loi " informatique et libertés". Ainsi toute création de fichiers comportant un traitement de données nominatives doit au préalable faire l'objet d'une déclaration ou d'une demande d'avis auprès de la Commission Nationale Informatique et Libertés (CNIL). Dans ce cadre, l'utilisateur s'adressera au correspondant « informatique et libertés » de l'Université.

4. Utilisation de logiciels

Il est rappelé que l'utilisateur ne peut installer un logiciel qu'après avis du service informatique compétent.

L'utilisation des logiciels mis à disposition est soumise aux règles de la propriété intellectuelle et industrielle :

- l'utilisation, la diffusion, la duplication de logiciels, pré installés ou non, doit se faire en accord avec la licence d'utilisation de chaque logiciel.

L'utilisateur de l'ordinateur ne devra en aucun cas :

- installer des logiciels à caractère ludique
- contourner les restrictions d'utilisation des logiciels mis à sa disposition.
- installer à demeure des programmes ou copies de programmes non fournis par l'Établissement
- installer ou développer des programmes qui s'auto dupliquent ou s'attachent à d'autres programmes, et ce afin de prévenir la contamination par d'éventuels virus informatiques.
- installer ou développer des programmes qui peuvent aboutir à un mauvais fonctionnement de l'ensemble du système installé sur le poste informatique
- contribuer à la diffusion de « SPAM » et autres messages du même type.

5. Utilisation des moyens informatiques

Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il informe le service informatique de toute anomalie constatée. L'utilisateur doit s'efforcer de n'occuper que la quantité d'espace disque qui lui est strictement nécessaire et d'utiliser de façon optimale les moyens de compression des fichiers dont il dispose. L'utilisation des ressources doit être rationnelle et loyale afin d'en éviter la saturation.

Tout ordinateur propre à un département, laboratoire ou service, doit être connecté au réseau par l'intermédiaire d'un informaticien de l'Université. Ce dernier s'assure en particulier que les règles de sécurité sont bien respectées.

Chaque utilisateur s'engage à ne pas entraver le bon fonctionnement des logiciels anti-virus. Tout utilisateur utilisant son propre matériel informatique doit veiller à faire la mise à jour régulière de l'anti-virus.

Un utilisateur ne doit jamais quitter un poste de travail en libre service sans se déconnecter.

Les utilisateurs sont informés que pour des raisons d'administration des systèmes et de gestion de la sécurité, les administrateurs systèmes ont la possibilité de réaliser des interventions à distance pour assurer la maintenance corrective ou évolutive des Systèmes d'Information mis à leur disposition ainsi que pour préserver ou renforcer des mesures de sécurité.

Le système d'information ainsi que l'ensemble des moyens de communication peuvent donner lieu à

surveillance et contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Les administrateurs doivent impérativement respecter la confidentialité des fichiers des utilisateurs.

Ces systèmes ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'une réquisition judiciaire et après accord du Président de l'Université, ces fichiers peuvent être mis à la disposition ou transmis aux autorités compétentes.

6. Contrôle des pages Web hébergées sur le serveur de l'université

L'université se réserve le droit de contrôler le contenu de toute page Web hébergée sur ses serveurs en vue de s'assurer du respect des dispositions législatives et réglementaires pertinentes.

L'université se réserve le droit de suspendre l'usage du service d'hébergement des pages Web par un utilisateur en cas de non-respect de la charte et notamment dans l'hypothèse où l'utilisateur aurait diffusé sur ses pages Web un contenu manifestement illicite.

7. Dispositions particulières concernant la messagerie électronique

7.1 Gestion des boîtes aux lettres

L'université de Lille 2 met à la disposition des utilisateurs une boîte aux lettres professionnelle ou pédagogique personnelle qui leur permet d'émettre et de recevoir des messages électroniques.

La taille de celle-ci est limitée.

Les utilisateurs sont avertis que dans le cas où la boîte aux lettres atteint sa taille maximum, tout nouveau message reçu sera rejeté avec la mention « quota atteint ». Il appartient à chaque utilisateur de gérer correctement l'archivage et la suppression de ses messages.

7.2 Contenu des messages électroniques

Les messages électroniques permettent d'échanger des informations à vocation professionnelle ou pédagogique liées à l'activité directe de l'université. Les utilisateurs s'engagent à adopter un comportement loyal et digne et à protéger l'image du service public de l'Education Nationale.

Il est rappelé que les messages à caractère injurieux, raciste, discriminatoire, insultant, dénigrant, diffamatoire, dégradant, ou susceptibles de révéler les opinions politiques, religieuses, philosophiques, les mœurs, l'appartenance syndicale ou la santé des personnes, ou encore de porter atteinte à leur vie privée ou à leur dignité ainsi que les messages portant atteinte à l'image, la réputation ou à la considération du service public de l'Education Nationale sont interdits. Toute utilisation de la messagerie à des fins commerciales est également strictement interdite.

7.3 Emission des messages

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter la diffusion de messages en masse, l'encombrement inutile de la messagerie et une dégradation des temps de réponse.

L'utilisateur devra s'abstenir de créer un fichier joint au message comportant des informations nominatives qui ne seraient pas en conformité avec les déclarations faites auprès de la Commission Nationale de l'Informatique et des Libertés.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose au retrait de son compte informatique, ainsi qu'aux poursuites disciplinaires et pénales, prévues par les textes législatifs et réglementaires en vigueur.

8. Sanctions

8.1 Sanctions internes :

En cas de non-respect des règles définies dans la présente charte, le Président de l'Université, juridiquement responsable pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des utilisateurs en fonction de leur statut, refuser ou limiter le droit d'accès aux ressources informatiques de l'Université.

Il est rappelé que tout comportement fautif est susceptible d'être sanctionné disciplinairement dans le cadre des procédures prévues par le statut particulier de l'utilisateur.

8.2 Sanctions pénales :

L'Université est tenue par la loi de signaler 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.

8.3 Sanctions civiles :

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

9. Liste informative des principaux textes se rapportant à la sécurité des systèmes informatiques et à la protection des personnes :

9.1. Infractions prévues par le Nouveau Code pénal

9.1.1. Crimes et délits contre les personnes

· Atteintes à la personnalité:

(Respect de la vie privée art. 9 du code civil)

- Atteintes à la vie privée (art. 226-1 al. 2 ; 226-2 al. 2, art.432-9 modifié par la loi n° 2004-669 du 9 juillet 2004)

- Atteintes à la représentation de la personne (art. 226-8)

- Dénonciation calomnieuse (art. 226-10)

- Atteinte au secret professionnel (art. 226-13)

- Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-16 à 226-24, issus de la 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

· Atteintes aux bonnes mœurs et mineurs :

(art. 227-23 ; 227-24 et 227-28). Loi 2004- 575 du 21 juin 2004 (LCEN)

9.1.2. Crimes et délits contre les biens

· Escroquerie (art. 313-1 et suite)

· Atteintes aux systèmes de traitement automatisé de données (art. 323-1 à 323-7 modifiés par la loi n° 2004-575 du 21 juin 2004).

9.1.3 Cryptologie

· Art. 132-79 (inséré par loi n° 2004-575 du 21 juin 2004 art. 37)

9.1.4 Atteinte au secret des correspondances

(art. 226-15 et art.432.9)

9.2. Infractions de presse (loi 29 juillet 1881, modifiée)

· Provocation aux crimes et délits (art.23 et 24)

- Apologie des crimes contre l'humanité (art. 24)
- Apologie et provocation au terrorisme (art. 24)
- Provocation à la haine raciale (art. 24)
- « Négationnisme »: contestation des crimes contre l'humanité (art. 24 bis)
- Diffamation (art. 30.31 et 32)
- Injure (art. 33)

9.3 Infraction au Code de la propriété intellectuelle

- Contrefaçon d'une oeuvre de l'esprit (y compris d'un logiciel) (art. 335-2 modifié par la loi n° 2004-204 du 9 mars 2004, art. 34 - et art. 335-3)
- Contrefaçon d'un dessin ou d'un modèle (art. L521-4 modifiée par la loi n° 2004-204 du 9 mars 2004, art. 34)
- Contrefaçon de marque (art. L716-9 - modifié par la loi n° 2004-204 du 9 mars 2004, art. 34 -et suivants)

9.4. Participation à la tenue d'une maison de jeux de hasard (« cyber-casino »)

- Art.1 de la loi du 12 juillet 1983, modifié par la loi du 16 décembre 1992

10. Entrée en vigueur de la charte

La présente charte adoptée par le Conseil d'Administration en sa séance du 30 juin 2005 prend effet dès sa date de publication sur le site du Centre de Ressources Informatique de l'Université. Aucun compte, aucune adresse électronique ne sera délivrée sans approbation de la présente charte par l'utilisateur.