UNIVERSITÉ D'ARTOIS

**CHARTE REGISSANT L'USAGE
DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION
PAR LES USAGERS DE L'UNIVERSITE D'ARTOIS**

Annexe II

ANNEXE RELATIVE A L'USAGE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION PAR LES PERSONNELS DE L'UNIVERSITE D'ARTOIS

Cette annexe s'applique à toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut, notamment tout agent titulaire ou non titulaire concourant à l'exécution des missions de l'Université.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent et notamment la sécurité, la performance des traitements et la conservation des données personnelles.

Engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents portés à sa connaissance. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.

L'utilisateur a une responsabilité particulière dans l'utilisation qu'il fait des ressources mises à sa disposition par l'Université et des opérations réalisées à partir de son compte. Il s'engage à ne pas quitter son poste de travail sans avoir correctement fermé sa session ou l'avoir verrouillée. En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

Article I. Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'établissement ainsi qu'à l'ensemble des utilisateurs.

Les utilisateurs ayant des fonctions spécifiques sur les systèmes d'information sont soumis à des règles complémentaires et spécifiques précisant leurs obligations particulières *(cf annexe III Charte des Administrateurs)*.

Article II. Conditions d'utilisation des systèmes d'information

A - Utilisation professionnelle / privée

Les communications électroniques (messagerie, internet …) sont des outils de travail ouverts à des usages professionnels administratifs et pédagogiques, ils peuvent constituer le support d'une communication privée.

L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

B - Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer cette continuité, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux systèmes d'information, notamment en fournissant un accès administrateur à son ordinateur. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies quant à elles par l'Université.

Article III. Principes de sécurité

A - Règles de sécurité applicables

L'Université met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs. Ces derniers sont informés que les mots de passe constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des systèmes d'information mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe,
- de garder strictement confidentiel(s) son (ou ses) mot(s) de passe et ne pas les dévoiler à un tiers,
- de respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre utilisateur, ni chercher à les connaître.

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son mot de passe, il devra procéder dès que possible, au changement de ce dernier ou en demander la modification à l'administrateur. Le bénéficiaire de la communication du mot de passe ne peut le communiquer à son tour à un tiers, ni l'utiliser en dehors de circonstances exceptionnelles à l'origine de la communication.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions:

- **de la part de l'Université :**
  - Veiller à ce que les ressources sensibles ne soient pas accessibles en cas d'absence (en dehors des mesures de continuité mises en place par la hiérarchie).
  - Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.
- **de la part de l'utilisateur :**
  - Si l'utilisateur ne bénéficie pas d'une habilitation explicite, il doit s'interdire d'accéder ou tenter d'accéder à des ressources du système d'information, même si cet accès est techniquement possible,
  - Ne pas connecter directement aux réseaux locaux des matériels non confiés ou non autorisés par l'Université,
  - Ne pas installer, télécharger ou utiliser sur le matériel de l'université de logiciels ou progiciels sans autorisation explicite, ne pas dupliquer de logiciel sous licence, ni installer de logiciels, sans s'assurer que l'Université dispose des licences nécessaires.
  - Se conformer aux dispositifs mis en place par l'Université pour lutter contre les virus et les attaques par programmes informatiques.

B - Devoirs de signalement et d'information

L'Université doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information. L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté, ou de toute anomalie découverte telle une intrusion dans le système d'information, etc... Il signale également à la personne responsable du site toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation.

C - Mesures de contrôle de sécurité

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'Université se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition,
- qu'une maintenance à distance est précédée d'une information à l'utilisateur,
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire sera isolée, le cas échéant supprimée.

L'université informe l'utilisateur que le système d'information fait l'objet d'une surveillance et d'un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus. Les administrateurs en charge des opérations de contrôle sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

Article IV. Communications électroniques

A - Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de l'Université. Elle est un outil de travail ouvert à des usages professionnels administratifs et pédagogiques.

1 - Adresses électroniques

L'Université s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie. L'adresse électronique nominative est attribuée à un utilisateur qui peut autoriser à son initiative et sous sa responsabilité, l'accès de tiers à sa boîte à lettres.

Une adresse électronique fonctionnelle ou organisationnelle peut être mise en place si elle est exploitée par un service ou un groupe d'utilisateurs. La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe « d'utilisateurs » relève de la responsabilité exclusive de l'Université d'Artois : ces adresses ne peuvent être utilisées sans autorisation expresse.

2 - Contenu des messages électroniques

Les messages électroniques permettent d'échanger principalement des informations à vocation professionnelle liées à l'activité directe de l'Etablissement. En toutes circonstances, l'utilisateur doit adopter un comportement responsable et respectueux des dispositions contenues dans la présente charte. Sont interdits les messages comportant des contenus à caractère illicite, quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (cf. annexe juridique).

3 - Emission et réception 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 les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

4 - Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1369 – 1 et 1369 – 11 du code civil. L'utilisateur doit en conséquence être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

5 - Stockage et archivage des messages.

Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve. A ce titre, il doit se conformer aux règles définies dans la présente charte.

B - Internet

Il est rappelé que le réseau internet est soumis à l'ensemble des règles de droit en vigueur. L'accès à ce réseau n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'université.

L'utilisation de la technologie internet (par extension intranet et extranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'université.

L'université met à la disposition de l'utilisateur un accès internet chaque fois que cela est possible. Internet est un outil de travail ouvert à des usages professionnels (administratifs, pédagogiques et de recherche), conformément aux dispositions légales et au regard de la mission éducative de l'Université.

L'Université se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

C - Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur le réseau internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article V. L'université se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'institution, code malicieux, programmes espions...) En particulier, l'utilisateur s'engage à ne pas tenter d'utiliser de logiciels de type peer-to-peer (kazaa, skype, etc...).

L'université est dans l'obligation légale de mettre en place un système de journalisation[1] des accès internet, de la messagerie et des données échangées.

Article V. Respect de la propriété intellectuelle

L'université rappelle que l'utilisation des moyens et ressources informatiques implique le respect des lois concernant la propriété intellectuelle et les droits d'auteurs.

Article VI. Déclaration des traitements automatisés de données

Tout traitement automatisé de données doit faire l'objet d'une déclaration préalable auprès du Correspondant Informatique et Libertés (C.I.L.) de l'Université.

[1] Conservation des informations techniques de connexions telle que l'heure d'accès, l'adresse IP de l'utilisateur.