UNIVERSITÀ DI CORSICA - PASQUALE PAOLI

CHARTE INFORMATIQUE DES PERSONNELS ET ETUDIANTS DE L'UNIVERSITE DE CORSE PASCAL PAOLI

1. Préambule

La présente charte a pour objet de formaliser les règles de déontologie et de sécurité que l' «utilisateur» s'engage à respecter en contrepartie de la mise à disposition des ressources informatique de l'institution.

Cette charte est portée à la connaissance des « utilisateurs ».

Par « utilisateur », on entend : toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux moyens informatiques et de télécommunications quel que soit son statut et notamment :

- Les agents titulaires et non titulaires concourant à l'exécution des missions du service public de l'éducation;
- Le personnel des prestataires de service dont le contrat passé avec le ministère ou le service concerné le prévoit expressément ;
- Les étudiants

Et plus généralement toute personne ayant accès aux systèmes d'information relevant du ministère chargé de l'Education nationale.

La charte est complétée par un Guide Technique Type de l' « utilisateur » et une Annexe Juridique de l' « utilisateur » qui définissent respectivement les principales règles pratiques et juridiques de mise en œuvre des règles permanentes et générales figurant dans la présente Charte. Ces guides sont en ligne sur l'ENT de l'Université de Corse.

La Charte définit le comportement loyal, respectueux et responsable que chacun s'oblige à adopter à l'occasion de l'utilisation des ressources informatiques de l'institution.

L'utilisation du système d'information suppose le respect des règles visant à assurer la sécurité, la performance des traitements, la préservation des données confidentielles et le respect des dispositions légales et règlementaires qui s'imposent.

Tout « utilisateur » est responsable, en tout lieu, de l'usage qu'il fait des ressources informatiques, de télécommunications et des réseaux auxquels il a accès.
L'administration est tenue de respecter la vie privée de ses agents.

2. Champ d'application

2.1 Périmètre

Les règles de déontologie et de sécurité figurant dans la présente Charte, celles définies par le Guide Technique Type de l' « utilisateur », de même que l'obligation de respecter la législation en vigueur s'appliquent à l'ensemble des « utilisateurs ».

Les « administrateurs » des systèmes d'information sont soumis en qualité d' « utilisateur » à la présente Charte et seront signataires d'une Charte spécifique liée à leurs missions professionnelles.

2.2 Systèmes d'information

Il s'agit de l'ensemble des moyens matériels, logiciels, applications et réseaux de télécommunications (Réseau Privé Virtuel, Réseau Téléphonique Commuté, etc.) pouvant être mis à disposition de l' « utilisateur », y compris via l'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portables, etc.

3. Destination des systèmes d'information

3.1 Utilisation professionnelle / privée

Les moyens informatiques mis à disposition de l' « utilisateur » sont prioritairement à usage professionnel.

L'utilisation à des fins privées doit être non lucrative et limitée tant dans la fréquence que dans la durée, conformément aux conditions et limites figurant dans la présente Charte. En outre, ce type d'usage ne doit avoir pour effet de nuire à la qualité de son travail ni au temps qu'il y consacre, ni au bon fonctionnement du service.

En tout état de cause, l' « utilisateur » est soumis au respect des obligations résultant de son statut ou de son contrat ainsi qu'aux obligations qui lui incombent en raison de la nature même du service public de l'éducation (notamment neutralité politique, philosophique ou religieuse) ou de ses fonctions.

En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des systèmes d'information doit demeurer négligeable au regard des coûts d'exploitation globaux.

Il appartient à l' « utilisateur » de procéder au stockage de ses données à caractère privée (messages, lettres, carnets d'adresses etc.) dans un espace de données nommé « privé », espace qui ne sera alors pas (systématiquement) inclus dans les sauvegardes. Toutes les informations ne se trouvant pas dans cet espace privé sont réputées professionnelles.

Ainsi, la sauvegarde régulière incombera à l' « utilisateur », sous sa seule responsabilité.

3.2 Utilisation des ressources des systèmes d'information

Les ressources matérielles nomades mises à la disposition de l' « utilisateur » par l'administration, doivent faire l'objet d'une attestation de remise signée par l' « utilisateur ».

L' « utilisateur » a obligation de préservation du matériel qui lui est confié.

L' « utilisateur » qui souhaitera être administrateur de sa machine devra signer la charte de l' « utilisateur » administrateur. Dans ce cas, l'Université se dégage toute responsabilité concernant l'utilisation de cette machine.

3.3 Gestion des départs

Il appartient à l' « utilisateur », lors de son départ définitif du service ou de l'établissement, de détruire son espace « privé »..

La responsabilité de l'administration ne pourra être engagée quant à la conservation et la confidentialité de l'espace privé d'un « utilisateur » quittant le service ou l'établissement.

4. Sécurité

4.1 Règles de sécurité

Les niveaux d'accès ouverts à l' « utilisateur » sont définis en fonction du « profil » qui est établi pour lui selon les critères propres à son statut, sa mission, la nature de son poste et ses besoins professionnels.

La sécurité des moyens informatiques mis à la disposition de l' « utilisateur » lui impose :

- de respecter les consignes de sécurité et notamment les règles relatives à la définition et aux changements des mots de passe qui sont précisés dans le Guide Technique Type de l' « utilisateur » ;
- de respecter la gestion des accès, en particulier ne pas utiliser les nom et mot de passe d'un autre « utilisateur », ni chercher à connaître ces informations ;
- de garder strictement confidentiels ses mots de passe et ne pas les dévoiler à un tiers.

Si pour des raisons exceptionnelles et ponctuelles, un « utilisateur » se trouvait dans l'obligation de communiquer son mot de passe, il devrait procéder, dès qu'il en a la possibilité, au changement de ce dernier ou en demander la modification à « l'administrateur » du réseau. 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 la circonstance exceptionnelle à l'origine de la communication.

L' « utilisateur » est informé que les mots de passe constituent une mesure de sécurité destinée à éviter les utilisations malveillantes ou abusives. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

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

- de verrouiller son poste de travail en cas d'absence et/ou d'utiliser les économiseurs d'écran avec mot de passe afin de préserver l'accès à son poste de travail ;
- d'avertir immédiatement ou dans le délai le plus court , sa hiérarchie de tout dysfonctionnement constaté, de toute anomalie découverte telle une intrusion dans le système d'information, etc. ;
- de ne pas modifier l'équipement qui lui est confié en conformité avec les dispositions en vigueur de l'établissement ;
- de ne pas connecter aux réseaux locaux des matériels non confiés par l'institution ;
- de ne pas installer, télécharger ou utiliser sur les matériels informatiques de logiciels ou progiciels sans qu'une licence d'utilisation appropriée n'ait été souscrite ;
- de s'interdire d'accéder ou tenter d'accéder à des ressources ou programmes informatiques pour lesquels l' « utilisateur » ne bénéficie pas d'une habilitation expresse : l' « utilisateur » doit limiter ses accès aux seules ressources pour lesquelles il est expressément habilité à l'exclusion de toutes autres, même si cet accès est techniquement possible ;
- de signaler à la Personne Juridiquement Responsable (PJR) tout accès à une ressource informatique qui ne corresponde pas à son habilitation : l' « utilisateur » s'interdit toute divulgation de cette possibilité d'accès.

L' « utilisateur » est informé que pour des actions de maintenance corrective ou évolutive, l'administration a la possibilité de réaliser des interventions, le cas échéant à distance, sur les ressources mises à sa disposition.
L' « utilisateur » est préalablement informé de ce type d'opérations.

4.2 Mesures de contrôle de la sécurité

Le système d'information ainsi que l'ensemble des moyens de communication peuvent donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Les personnels en charge de ces opérations sont soumis au secret professionnel et ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction, en particulier lorsque ces informations sont couvertes par les secrets de correspondances ou relèvent de la vie privée de l' « utilisateur » et lorsque ces informations ne remettent pas en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du service.

5. Sécurité anti-virale

L' « utilisateur » doit se conformer aux règles liées à la mise en œuvre au sein de l'institution, des dispositifs de lutte contre les virus et attaques logiques informatiques qui sont précisées dans le Guide Technique Type de l' « utilisateur ».

L' « utilisateur » est informé que toute information bloquante ou présentant une difficulté technique d'acheminement à son destinataire, peut être isolée voire détruite.

Les services réseaux pourront être arrêtés en cas de difficultés majeurs.

6. Message électronique

L'administration met à la disposition de l' « utilisateur » une boîte à lettres professionnelle nominative qui lui permet d'émettre et de recevoir des messages électroniques.

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail au sein de l'institution et de la politique de mutualisation de l'information.

L'élément nominatif de l'adresse de la messagerie qui constitue le prolongement de l'adresse administrative, n'a pas pour effet de retirer le caractère professionnel de la messagerie.

6.1 Boîte aux lettres

Chaque « utilisateur » peut autoriser, à son initiative et sous sa responsabilité, l'accès par des tiers à sa boîte de réception.
L'attribution de boîtes générales fonctionnelles ou organisationnelles par service ou groupe d' « utilisateur » est possible.

Les listes de diffusion institutionnelles désignant une catégorie ou un groupe d' « utilisateurs » ne peuvent être mises en place et utilisées que sous la condition d'une autorisation de l'institution.

6.2 Contenu des messages électroniques

Les messages électroniques permettent d'échanger des informations à vocation professionnelle liées à l'activité directe de l'institution. En toutes circonstances, l' « utilisateur » doit adopter un comportement loyal et digne.

Tout message à caractère privé, reçu ou émis, doit comporter une mention particulière explicite indiquant le caractère privé dans la zone « objet ». A défaut, le message sera réputé professionnel sauf s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : les termes sont précisés dans le Guide Technique Type de l' « utilisateur ».

Sont interdits les messages à caractère injurieux, racistes, discriminatoire, insultant, dénigrant, diffamatoire, dégradant ou susceptibles de révéler les opinions politiques, religieuses, philosophiques, les mœurs, l'appartenance syndicale, 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. Le non respect de ces dispositions pourra faire l'objet de procédures disciplinaires.

6.3 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 limités aux seuls destinataires concernés afin d'éviter la diffusion de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

6.4 Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, constituer une preuve ou un commencement de preuve.

L' « utilisateur » doit en conséquence être vigilant sur la nature des messages électroniques qu'il échange au même titre que les courriers traditionnels.

6.5 Stockage et archivage des messages électroniques

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 notamment se conformer aux règles définies dans la présente Charte et dans le Guide Technique Type de l' « utilisateur » pour l'utilisation des technologies de l'information et de communications en vigueur.

6.6 Gestion des absences

En cas d'absence d'un « utilisateur », toute mesure visant à assurer la continuité du service pourra être mise en œuvre par la hiérarchie.

7. Web – Internet et traces

L'accès à Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution.
Les règles de sécurité spécifiques applicables au réseau Internet (Web) sont précisées dans le Guide Technique Type de l' « utilisateur ». Il est rappelé que le réseau Internet se trouve soumis à l'ensemble des règles de droit.

L' « utilisateur » qui dispose d'un accès au réseau Internet est informé des risques et limites inhérents à son utilisation.

L'institution a mis en place un système permettant d'assurer la traçabilité des accès internet et/ou données échangées. Elle se réserve le droit de procéder à un filtrage des sites, au contrôle a posteriori des sites, des pages visitées et durées des accès correspondants.

Les traces correspondantes aux connexions et aux sites Internet accédés par l' « utilisateur » sont conservés et font l'objet d'une déclaration auprès de la CNIL.

8. Téléchargements – logiciels

Le téléchargement de fichiers, notamment de sons et d'images, depuis le réseau Internet est autorisé dans le respect des droits de la propriété intellectuelle telle qu'elle est définie à l'article 10 mais doit correspondre à l'activité professionnelle de l' « utilisateur ».

Cependant, l'administration se réserve le droit de limiter a priori le téléchargement de certains fichiers pouvant se révéler volumineux ou comporter des virus susceptibles d'altérer le bon fonctionnement du système d'information de l'institution.

9. Confidentialité – discrétion

Chaque « utilisateur » a une obligation de confidentialité et de discrétion à l'égard des informations et documents électroniques à caractère confidentiel auxquels il a accès dans le système d'information.

Le respect de cette confidentialité implique notamment :

- de veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations ;
- de respecter les règles d'éthique professionnelle et de déontologie, ainsi que l'obligation de réserve et le devoir de discrétion.

10. Propriété intellectuelle

L'utilisation des moyens informatiques implique le respect des droits de propriété intellectuelle de l'institution, de ses partenaires et plus généralement de tous tiers titulaires de tels droits.
En conséquence, chacun doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier et utiliser les logiciels, bases de données, pages web, texte, image, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

11. Respect de la loi informatique et libertés

L' « utilisateur » est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données nominatives conformément à la loi n°78-17 du 06 janvier 1978 dite « Informatique et Libertés » modifiée par la loi n°2004-801 du 06 août 2004, la loi n°2011-334 du 29 mars 2011 et la loi n°2011-525 du 17 mai 2011.

Par données nominatives, il y a lieu d'entendre, les informations qui permettent – sous quelque forme que ce soit – directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi n°78-17 du 06 janvier 1978 modifiée par la loi n°2004-801 du 06 août

2004, la loi n°2011-334 du 29 mars 2011 et la loi n°2011-525 du 17 mai 2011.

En conséquence, tout « utilisateur » souhaitant procéder à un tel traitement devra en informer préalablement la cellule CIL (Correspondants Informatique et Liberté) de l'Université de Corse qui prendra les mesures nécessaires au respect des dispositions légales. Cette cellule a été mise en place en mai 2008, elle est composée de Pascale Urbani (CRI, urbani@univ-corse.fe, 0495450060) et Marie-Dominique Giamarchi (Service Juridique, mdgiamarchi@univ-corse.fr, 0495450140).

Par ailleurs, conformément aux dispositions de la loi informatique et libertés n°78-17 du 06 janvier 1978 modifiée par la loi n°2004-801 du 06 août 2004, la loi n°2011-334 du 29 mars 2011 et la loi n°2011-525 du 17 mai 2011, chaque « utilisateur » dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des Systèmes d'Information.
Ce droit s'exerce auprès de la Direction des Affaire juridiques.

12. Limitation des usages

En cas de non-respect des règles définies dans la présente Charte et des modalités définies dans le Guide Technique type de l' « utilisateur », la « Personne Juridiquement Responsable » pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Par « Personne Juridiquement Responsable » on entend : toute personne ayant la responsabilité de représenter le Ministre (recteur, inspecteur d'académie) ou un établissement d'enseignement scolaire, supérieur et de recherche (président d'université, chef d'établissement, etc.).

Tout abus dans l'utilisation des moyens informatiques mis à la disposition de l' « utilisateur » à des fins extra-professionnelles, est passible de sanctions.

13. Entrée en vigueur de la charte

La présente Charte est annexée au règlement intérieur de l'Université de Corse Pascal PAOLI. A défaut de règlement intérieur, la Charte a valeur de règlement intérieur pour ce qui concerne l'usage des Systèmes d'Information.

Le présent document annule et remplace tous autres documents ou chartes afférents à l'utilisation des Systèmes d'Information.

Pour la Direction de l'Université de Corse,

Fait à Corte, le
Le Président, Paul-Marie Romani

GUIDE TECHNIQUE TYPE DE L' « UTILISATEUR »

UNIVERSITE DE CORSE PASCAL PAOLI

1. Préambule

Le présent Guide Technique Type de l' « utilisateur » a pour objet de définir les procédures techniques devant être appliquées par toute personne utilisant les moyens informatiques et de télécommunications de l'Université de Corse.

Il complète la Charte des Personnels de l'Education nationale régissant l'usage des technologies de l'information et de la communication en vigueur au sein de l'Université de Corse.

Les « utilisateurs » sont informés que la violation des procédures régissant l'accès et l'utilisation des Systèmes d'Information et de télécommunications mis à leur disposition par l'Université de Corse est susceptible d'entraîner des sanctions.

2. Champ d'application

Le présent Guide Technique Type, pris en application de la Charte des personnels de l'Université de Corse s'applique aux « utilisateurs » et aux moyens informatiques et de télécommunication de l'Université de Corse tels que définis dans la Charte des Personnels de l'Université de Corse

3. Procédure de Sécurité

3.1 Règles de définition et de gestion des mots de passe

Chaque « utilisateur » doit veiller au respect de la sécurité liée aux mots de passe permettant l'accès à son ou ses environnements.

A cet égard, chaque « utilisateur » :

- doit choisir un mot de passe sûr, n'ayant aucun lien avec l'environnement familier de l' « utilisateur » ;
- doit changer de mot de passe régulièrement, si les applications le permettent ;

- ne doit pas écrire son mot de passe sur un support facilement accessible.

Les mots de passe choisis par les « utilisateurs » sont constitués de 7 caractères alphanumériques au minimum dont au moins un chiffre ou un caractère spécial.

Les mots de passe devront être changés selon une périodicité de 6 mois au maximum.

Chaque « utilisateur » est personnellement responsable du mot de passe qu'il a choisi.

A ce titre, il s'engage à :
- garder confidentiel ses mots de passe ;
- changer immédiatement ses mots de passe en cas de doute sur sa confidentialité.

3.2 Paramétrage des postes de travail

Les postes de travail de l' « utilisateur » constituent un outil qui doit être protégé des intrusions.

A cet égard, il convient de :
- paramétrer la mise en veille automatique des postes de travail avec demande du mot de passe pour la réactivation du poste après 15 minute d'inactivité ;
- de ne pas se connecter au réseau ou ouvrir des sessions applicatives inutilement ;
- d'effectuer une déconnexion des serveurs réseaux et quitter les applications actives avant de quitter son poste de travail.

4. Messagerie électronique

4.1 Message à caractère privé

Tout message à caractère strictement privé, reçu ou émis, doit comporter en objet la mention « Privé » ou tout autre terme indiquant sans ambigüité le caractère privé du message.

Tout message ne comportant pas cette mention est réputée être un message professionnel.

L'envoi ou la réception de pièces jointes est autorisé à la condition d'être limité à un usage professionnel.

4.2 Caractéristiques et limitations de la messagerie électronique

Les messages envoyés ou reçus font l'objet d'une limitation de taille particulière.

En cas de dépassement de la taille limite, le message est rejeté et l'émetteur reçoit un message de non distribution.

4.3 Stockage et archivage des messages électroniques

Chaque « utilisateur » est responsable de l'archivage et du classement des messages qu'il a relevés.

Le serveur de messagerie de l'Université de Corse étant sauvegardé quotidiennement, les messages stockés sur le serveur sont conservés.

Chaque « utilisateur » doit en conséquence organiser lui-même la conservation des éléments en décidant :
- du nombre de génération de sauvegarde et leur périodicité ;

- du choix des fichiers et messages conservés et de ceux qui sont détruits ;
- du lieu et de la durée de stockage.

L' « utilisateur » doit mettre en œuvre les moyens nécessaires à la conservation des messages qui pourraient être indispensables notamment en tant qu'élément de preuve.

4.4 Sécurité anti-virale

De manière générale, il est déconseillé d'ouvrir des fichiers, de quelque nature que ce soit en provenance d'un expéditeur inconnu.

En particulier, les fichiers compressés (extension en .zip par exemple) ou exécutables (extension en .exe par exemple) peuvent générer l'activation de virus informatiques, code malicieux etc., susceptibles d'entraîner des conséquences d'une extrême gravité pour l'Université de Corse.

Les « utilisateurs » sont informés que l'Université de Corse se réserve le droit de retenir, d'isoler et/ou de supprimer tout message à l'aide de moyens automatisés et ce, sans que ces messages n'aient été nécessairement ouverts, afin de vérifier qu'ils ne comportent pas de virus.

D'une manière générale les « utilisateurs » sont informés que tout message bloquant ou présentant une difficulté technique d'acheminement à son destinataire peut être détruit sur décision de la Direction des Systèmes d'Information.

Les « administrateurs » sont autorisés, en cas de difficultés majeures, à arrêter les services réseaux.

5. Web - Internet

Il est rappelé que l'accès à Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'Université de Corse.

Les « utilisateurs » ne doivent utiliser que les navigateurs sélectionnés et qualifiés par le Centre de Ressources Informatiques, dans le cadre du paramétrage et des seules extensions fournies par l'Université de Corse.

Pour des raisons de sécurité, tout abonnement souscrit chez un prestataire de services et nécessité par l'exercice de l'activité professionnelle d'un ou de plusieurs « utilisateurs », devra faire l'objet d'une concertation préalable avec le Centre de Ressources Informatiques. Il en est de même pour l'accès à des sites Web payants.

6. Matériel nomade

6.1 Les principes de précaution

Toute personne de l'Université de Corse, à qui a été confié exclusivement dans le cadre de ses activités professionnelles un équipement de type appareil photo numérique, caméscope, téléphone portable, ordinateur portable etc., doit veiller à le protéger.

En cas de non utilisation, le matériel doit être rangé dans un endroit sécurisé.

Aucun matériel non confié par l'Université de Corse ne doit être connecté au réseau local de l'Université de Corse.

Par ailleurs, l' « utilisateur » doit veiller particulièrement à ne pas exposer l'équipement confié à la chaleur, à l'humidité, ni le laisser sans surveillance.

6.2 Vol

En cas de vol de l'équipement fourni, une déclaration doit être effectuée sans délai à la gendarmerie la plus proche avec copie adressée à l'Université de Corse.

Toute déclaration volontairement fausse est passible de sanctions disciplinaires et/ou de poursuites pénales.

6.3 Perte

En cas de perte de l'équipement confié, une déclaration détaillée doit être adressée à l'Université de Corse.

6.4 Détérioration

En cas de détérioration du matériel portable, celui-ci doit être retourné au responsable de l'Université de Corse accompagné du détail des circonstances dues à sa détérioration.

7. Evolution du présent guide

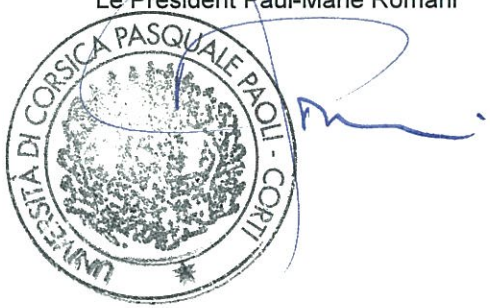
Le présent Guide Technique Type de l' « utilisateur » est rédigé dans l'intérêt de chacun des « utilisateurs » et manifeste la volonté de l'Université de Corse d'assurer un développement harmonieux et sécurisé de l'accès et de l'utilisation des moyens informatiques mis à disposition.

Le présent Guide Technique Type de l' « utilisateur » sera régulièrement mis à jour et il appartient à l' « utilisateur » de prendre connaissance de toutes nouvelles versions du Guide Technique Type qui seront portées à sa connaissance par le biais de la messagerie ou par Intranet.

Les « utilisateurs » devront veiller à se conformer aux dernières dispositions en vigueur.

Pour la Direction de l'Université de Corse,

Fait à Corte, le
Le Président Paul-Marie Romani



GUIDE JURIDIQUE DE L'UTILISATEUR

DES SYSTEMES D'INFORMATION

DE L'UNIVERSITE DE CORSE PASCAL PAOLI

ARTICLE I. PREAMBULE

Le présent guide juridique de l' « utilisateur » s'inscrit dans le cadre de la politique de sécurité du ministère de l'éducation nationale et du ministère de l'enseignement supérieur et de la recherche (dénommé ci-après « ministère »).

Le guide est pris en application des règles édictées dans la charte des personnels, dans le prolongement de laquelle il s'inscrit ; il la complète.

Il a pour objet d'exposer aux « utilisateurs », les principales règles légales applicables, de manière non exhaustive. Ces règles ne sont pas exclusives de celles qui s'imposent à tout agent public notamment en ce qui concerne l'obligation de neutralité (religieuse, politique et commerciale), de réserve, de discrétion professionnelle et de respect des secrets protégés par la loi.

Il a une vocation pédagogique.

ARTICLE II. LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Les données à caractère personnel font l'objet d'une protection légale particulière dont la violation expose son auteur à des sanctions pénales.

Les textes applicables en la matière sont les suivants :

- la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004, la loi n°2011-334 du 29 mars 2011 et la loi n°2011-525 du 17 mai 2011 ;
- la convention n°108 du conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;
- la directive n°95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Ces règles s'appliquent à l'ensemble des systèmes de traitement de l'information dès lors que cette information permet d'identifier un ou plusieurs individus

La loi du 6 janvier 1978 modifié par les lois n°2004-801, 2011-334 et 2011-525 a créé un dispositif juridique pour encadrer la mise en œuvre des « traitements automatisés de données à caractère personnel » et ouvrir aux individus un droit d'accès et de rectification sur les données les concernant détenues et gérées par des tiers.

Cette loi impose de procéder à une déclaration et/ou une demande d'avis auprès de la Commission Nationale de l'Informatique et des libertés (CNIL) préalablement à la mise en œuvre d'un tel traitement automatisé.

Toute personne auprès de laquelle sont collectées (oralement ou par écrit) des informations destinées à être mises en œuvre dans un système automatisé de traitement doit être informée :

- du caractère obligatoire ou facultatif de réponse ;
- des conséquences d'un défaut de réponse ;
- de l'identité des destinataires des informations ;
- de l'existence d'un droit d'accès et de rectification ;
- de l'identité du responsable du traitement ;
- des finalités du traitement auquel les données sont destinées.

Si les données sont destinées à être communiquées à des pays tiers à l'Union européenne, la personne doit recevoir une information sur ce point.

De même, si les données sont destinées à être utilisées à des fins de prospection, à être communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection, une information sur ce point doit lui être donnée, accompagnée d'une possibilité de s'y opposer (au moyen d'une case à cocher ou à cliquer notamment).

ARTICLE III. LA PROTECTION DES PERSONNES

Ainsi qu'il l'a été précédemment évoqué, les traitements automatisés d'informations à caractère personnel sont strictement règlementés par la loi du 6 janvier 1978 modifiée par les lois n°2004-801, 2011-334 et 2011-525. Les dispositions relatives aux personnes sont identiques à celles décrites pour les données à caractère personnel dans le point précédent.

La violation de la loi précitée entraîne des sanctions pénales.

ARTICLE IV. LA PROTECTION DES DROITS DE PROPRIETE INTELLECTUELLE

SECTION 4.01 LES REGLES DE PROTECTION DU DROIT D'AUTEUR

En vertu des règles du Code de la propriété intellectuelle, l'auteur d'une œuvre de l'esprit jouit sur cette œuvre du seul fait de sa création « d'un droit de propriété incorporel et exclusif opposable à tous ».

Cette disposition s'applique à toutes les œuvres de l'esprit quel qu'en soit le genre, la forme d'expression, le mérite ou la destination.

Sont notamment considérées comme des œuvres de l'esprit, au sens du Code de la propriété intellectuelle et en particulier de l'article L.112-2, les œuvres suivantes :

- les livres, brochures et autres écrits littéraires, artistiques et scientifiques ;
- les conférences, allocutions et autres œuvres de même nature ;
- les œuvres dramatiques ou dramatico-musicales ;
- les œuvres chorégraphiques, .. ;
- les œuvres musicales avec ou sans paroles :
- les œuvres cinématographiques et autres œuvres consistant dans des séquences animées d'images sonorisées ou non, dénommées ensemble œuvres audiovisuelles ;
- les œuvres de dessins, de peintures, d'architectures, de sculptures, de gravures, de lithographies ;
- les œuvres graphiques et typographiques ;
- les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie ;
- les œuvres d'art appliqué ;
- les illustrations, les cartes géographiques ;
- les logiciels, y compris le matériel de conception préparatoire...

Les actes de reproduction et de représentation des œuvres protégées en tout ou partie, par tout moyen et sous toute forme sont ainsi soumis à l'autorisation du ou des titulaire(s) des droits des œuvres.

L'utilisation de ces œuvres suppose donc une acceptation préalable du ou des titulaire(s) des droits.

L' « utilisateur » est donc informé qu'à défaut d'une autorisation expresse du/ou des titulaire(s) respectant les dispositions du Code de la propriété intellectuelle, il lui est interdit d'utiliser une telle œuvre.

A défaut, sa responsabilité civile et/ou pénale peut être engagée.

SECTION 4.02 LES REGLES DE PROTECTION DES LOGICIELS

Les logiciels sont protégés par le droit d'auteur.

Toute reproduction, adaptation et/ou distribution du logiciel n'est autorisé que sous réserve du consentement du titulaire des droits sur le dit logiciel.

L'étendue et les caractéristiques des droits conférés sont définies en général par des contrats de licence d'utilisation qui précisent les modalités selon lesquelles est autorisée l'utilisation des logiciels visés.

L'utilisation du logiciel, même à des fins d'essais, de démonstration de courte durée ou à des fins pédagogiques et à défaut d'autorisation expresse et écrite du titulaire des droits est en principe interdite.

L' « utilisateur » d'un logiciel s'expose à des sanctions civiles et pénales prévues et réprimées par le Code de la propriété intellectuelle lorsqu'il utilise un logiciel sans autorisation.

Afin de prévenir les risques liés à la contrefaçon de logiciel, une vigilance particulière des utilisateurs comme de leur autorité hiérarchique est indispensable.

Est un délit de contrefaçon puni par le Code de la propriété intellectuelle, (article L.335-3 du Code de la propriété intellectuelle) toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur ainsi que la violation des droits de l'auteur d'un logiciel.

SECTION 4.03 LES REGLES DE PROTECTION DES DONNEES ET DES BASES DE DONNEES

De la même façon, les données telles que les textes et, dès lors que ceux-ci présentent une certaine originalité, les images et les sons, sont protégés par le droit d'auteur.

L'autorisation écrite du titulaire des droits est ainsi nécessaire pour leur utilisation.

Le non-respect des dispositions relatives à la protection des droits de l'auteur sur ces données est constitutif de contrefaçon et il est donc civilement et/ou pénalement sanctionnable.

D'une manière générale, la difficulté à connaître précisément l'origine des données transmises et donc les droits y afférents, en particulier avec le développement des moyens d'échanges d'informations en réseau ouvert comme Internet, oblige les utilisateurs à la plus grande prudence.

On entend par bases de données un recueil d'œuvres de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou par tout autre moyen.

Les bases de données sont protégées par le Code de la propriété intellectuelle indépendamment de la protection dont peuvent bénéficier les données au titre du droit d'auteur contenu dans ladite base.

Les bases de données qui, par le choix ou les dispositions des matières, constituent des créations intellectuelles, bénéficient des dispositions du Code de la propriété intellectuelle.

Les bases de données peuvent faire l'objet d'une extraction ou d'une réutilisation partielle ou en totalité, conformément à l'article L.342-1 du code de la propriété intellectuelle.

L' « utilisateur » doit obtenir du producteur d'une base de données l'autorisation de :

- procéder à toute extraction par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle, du contenu de cette base sur un autre support, par tout moyen et sous toute forme que ce soit ;

- réutiliser tout ou partie de cette base de données.

A ce titre, un « utilisateur » des bases de données de l'institution ne saurait s'autoriser à utiliser à des fins privées par exemple, un fichier d'adresses, dont l'institution est propriétaire, et ne saurait le télécharger ou en faire toute utilisation contraire au Code de la propriété intellectuelle.

ARTICLE V. LA PROTECTION DES MARQUES

Le Code de la propriété intellectuelle protège « toute marque de fabrique, de commerce ou de service servant à distinguer les produits ou services d'une personne physique ou morale » (article L.711-1).

Peuvent être définis et utilisés à titre de marque, tous signes nominaux, figuratifs ou sonores, tels que les mots, assemblage de mots, nom patronymique, nom géographique, pseudonyme, lettre, chiffre, sigle, emblème, photographie, dessin, empreinte, logo ou la combinaison de certains d'entre eux.

Ces droits et leur protection sur une marque confèrent à son titulaire par un enregistrement, un droit de propriété sur cette marque.

L' « utilisateur » ne peut, sauf autorisation du propriétaire, reproduire, utiliser ou apposer une marque, ainsi qu'utiliser une marque protégée, supprimer ou modifier une marque régulièrement déposée.

Les « utilisateurs » s'interdisent donc, sauf autorisation expresse du propriétaire, toute reproduction ou usage ou apposition d'une marque ainsi que l'usage d'une marque reproduite pour des produits ou services identiques à ceux désignés dans l'enregistrement, la suppression ou la modification d'une marque.

L' « utilisateur » ne saurait utiliser une marque sur laquelle l'institution ne détient pas l'autorisation expresse d'utilisation dans le cadre de ses fonctions.

Il lui sera en outre interdit d'utiliser à des fins privées toute marque dont l'institution est titulaire.

ARTICLE VI. LA PROTECTION DES SYSTEMES D'INFORMATION

La protection des systèmes d'information est principalement mais non exclusivement organisée à travers les articles 323-1 et suivants du code pénal.

Ce dernier interdit notamment :

- l'accès illicite, c'est-à-dire toute introduction dans un système informatique par une personne non autorisée (article 323-1 du Code pénal) ;

La notion d'accès s'entend de tout système de pénétration tel que la connexion pirate tant physique que logique, l'appel d'un programme alors que l'on ne dispose pas d'habilitation, l'interrogation d'un fichier sans autorisation.

- le maintien frauduleux, c'est-à-dire le maintien sur le système informatique après un accès illicite et après avoir pris conscience du caractère « anormal » de ce maintien (article 323-3 du Code pénal) ;

Le maintien frauduleux est notamment caractérisé par des connexions, visualisations ou opérations multiples, alors que l'accédant a pris conscience que ce maintien est « anormal ».

- le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 susvisés (article 323-1)[1].

- l'entrave au système, c'est-à-dire toute perturbation volontaire du fonctionnement d'un système informatique 'article 323-2 du Code pénal) ;

L'entrave au système est appréhendée de manière extrêmement large car il suffit d'une influence « négative » sur le fonctionnement du système pour que le concept d'entrave soit retenu.

- l'altération des données, c'est-à-dire toute suppression, modification ou introduction de données « pirates », avec la volonté de modifier l'état du système informatique les exploitant et ce, quelle qu'en soit l'influence (article 323-1 du Code pénal) ;

Il en est ainsi pour les bombes logiques, l'occupation, la saturation de la capacité mémoire, la mise en place de codification, de barrage, ou tout autre élément retardant un accès normal.

Par ailleurs, la création doit impérativement adopter un comportement exempt de toute fraude car à défaut, il s'expose à de sévères sanctions pénales et disciplinaires.

ARTICLE VII. LE SECRET DES CORRESPONDANCES

L' « utilisateur » est informé qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende « le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance » (article 226-15 du Code pénal).

Il est également informé qu'est puni de trois ans d'emprisonnement et de 45 000 euros d'amende, « le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances » (article 432-9 du Code pénal).

ARTICLE VIII. LA RESPONSABILITE EN MATIERE DE TRANSMISSION DES INFORMATIONS

Les moyens informatiques mis à la disposition de l' « utilisateur » permettent l'accès à une communication et à une information importante et mutualisée.

Or, de tels moyens de communication ne doivent pas permettre de véhiculer n'importe quelle information ou donnée, dès lors que celle-ci serait susceptible de mettre en périls des mineurs.

Ainsi, le Code pénal, dans ses articles 227-23 et 227-24, sanctionne le fait de fabriquer, de transporter, de diffuser, par quelque moyen que ce soit et quel qu'en soit le support, un message à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, de trois ans d'emprisonnement et de 75 000 euros d'amende. Est également puni de cinq ans d'emprisonnement et de 75 000 euros d'amende, le fait de fixer, d'enregistrer ou de transmettre en vue de sa diffusion, l'image ou la représentation d'un mineur lorsque cette dernière présente un caractère pornographique.

Est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende, « le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit ».

ARTICLE IX. LE RESPECT DE LA VIE PRIVEE

SECTION 9.01 LE DROIT A LA VIE PRIVEE

Le principe est posé par l'article 9 du Code civil qui prévoit que 'chacun a droit au respect de sa vie privée'.

Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre ou autres, propres à empêcher ou à faire cesser une atteinte à l'intimité de la vie privée.

SECTION 9.02 DROIT A L'IMAGE

L' « utilisateur » est informé qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende, « le fait au moyen d'un procédé quelconque, de porter volontairement atteinte à l'intimité de la vie privée d'autrui :

1. En captant, enregistrant ou transmettant, sans le consentement de leur auteur des paroles prononcées à titre privé ou confidentiel ;
2. En fixant, enregistrant ou transmettant sans le consentement de celle-ci l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés ci-dessus ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé. (article 226-1 du Code pénal).

SECTION 9.03 LE DROIT DE REPRESENTATION

L' « utilisateur » est informé qu'est puni d'un an d'emprisonnement et de 15 000 euro d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention (article 226-1 du Code pénal).

ARTICLE X. LES REGLES DE PREUVE

Le principe est celui de la liberté de la preuve qui peut donc être rapportée par tout moyen.

A ce titre, l' « utilisateur » est informé qu'un message électronique peut constituer une preuve susceptible d'engager la responsabilité de l'institution ainsi que la sienne.

En effet, le code civil reconnaît à travers les articles 1316 à 1316-4 une valeur juridique à l'écrit sous forme électronique.

Il est nécessaire que chaque utilisateur respecte scrupuleusement la législation en vigueur car le non-respect de cette obligation est passible de sanctions pénales.

ARTICLE XI. L'OBLIGATION D'INFORMATION

L'article 40 du code de procédure pénale précise que « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.

Il s'agit là d'une obligation forte attachée à la personne d'un fonctionnaire qui est tenu d'informer mais également de communiquer les éléments dont il dispose auprès du procureur de la République lorsqu'il à connaissance d'un crime ou d'un délit.

Pour la Direction de l'Université de Corse,

Fait à Corte, le

le Président, Paul-Marie Romani