# Charte régissant l'usage du système d'information par les personnels et assimilés de L'Université de Toulouse II Le-Mirail

Sommaire

**Préambule**

Le "système d'information" recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'Université de Toulouse II Le Mirail.

L'informatique nomade, tels que les assistants personnels, les ordinateurs portables, les téléphones portables, ... est également un des éléments constitutifs du système d'information.

Par «institution», il faut entendre tout service ou composante pédagogique ou scientifique de l'UTM et de ses écoles internes.

Le terme d'«utilisateur» recouvre tout personnel ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut. Il s'agit notamment de :

- tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'enseignement supérieur et de la recherche en poste à l'université de Toulouse Le-Mirail ;
- tout prestataire[1] ayant contracté avec l'Université et conduit à devenir usager du SI de l'UTM dans le cadre de l'exécution de la prestation (y compris les sous-traitants)
- tout stagiaire ayant contracté une convention de stage avec l'un des services ou l'une des composantes de l'UTM
- toute personnalité invitée dans le cadre des missions du service public de l'enseignement supérieur et de la recherche par l'une des composantes ou l'un des services de l'université à intervenir sur l'un des campus de l'université de Toulouse II Le-Mirail.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données ainsi que les consignes de la charte RENATER.

La présente charte définit les règles d'usages et de sécurité que l'institution et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

La charte est accompagnée d'un guide juridique qui rappelle les dispositions législatives et réglementaires en vigueur pour son application. Ce guide peut être téléchargé à l'adresse « http://www.cnil.fr/la-cnil/actu-cnil/article/article/guide-pratique-pour-les-employeurs-et-les-salaries/ ». Elle pourra être complétée par des guides d'utilisation définissant les principales règles et pratiques d'usage.

Engagements de l'institution

L'université de Toulouse II Le-Mirail porte à la connaissance de l'utilisateur la présente charte.

L'université de Toulouse II Le-Mirail met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'université de Toulouse II Le-Mirail facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'institution est tenue de respecter l'utilisation résiduelle du système d'information à titre privé.

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 auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie[2].

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

[1] Le contrat devra prévoir expressément l'obligation de respect de la charte.
[2] Notamment le secret médical dans le domaine de la santé.

**Article I. Champ d'application**

En complément de la Charte régissant l'usage des réseaux de l'enseignement supérieur et de la recherche (RENATER), les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à L'université de Toulouse II - Le Mirail ainsi qu'à l'ensemble des utilisateurs.

Les usages relevant de l'activité des organisations syndicales pourront faire l'objet d'une charte spécifique.

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

**Section 2.01 Utilisation professionnelle / privée**

Les systèmes d'information (messagerie, internet,...) sont des outils de travail ouverts à des usages professionnels administratifs et pédagogiques.

Ils peuvent également constituer le support d'une communication privée dans les conditions décrites ci-dessous :

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. De manière générale, dans le souci de respecter la vie privée et en particulier le secret des correspondances, l'université s'engage à ne pas accéder au contenu de la messagerie d'un personnel. Toutefois, cet engagement ne saurait être maintenu si :

- l'activité des services est interrompue et que l'accès à la messagerie soit susceptible de permettre le rétablissement de l'activité.
- un problème technique ou de sécurité est constaté et que l'accès à la messagerie soit susceptible de résoudre le problème.

Rappel : seul les personnels de la DSi sont susceptibles de réaliser ces opérations. Ces personnels sont tenus à une obligation de confidentialité (Cf. la charte du personnel DSI).

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement[3] à cet effet ou en mentionnant le caractère privé sur la ressource[4]. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

L'utilisateur est responsable de son espace de données à caractère privé. 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 avec le responsable désigné au sein de l'institution.

L'utilisation des systèmes d'information à titre privé doit respecter la réglementation en vigueur. En particulier, la détention, diffusion et exportation d'images à caractère pédophile[5], ou la diffusion de contenus à caractère raciste ou antisémite[6] est totalement interdite.

Par ailleurs, eu égard à la mission éducative et scientifique de l'institution, la consultation de sites de contenus à caractère pornographique est strictement limitée aux activités de recherche dument reconnues

[3] Pour exemple, cet espace pourrait être dénommé "_privé_"
[4] Pour exemple, "_privé_nom_de_l_objet_» : l'objet pouvant être un message, un fichier ou toute autre ressource numérique.
[5] Article L 323-1 et s. du Code pénal
[6] Article 24 et 26bis de la Loi du 29 juillet 1881

**Section 2.02 Continuité de service : gestion des absences et des départs**

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition et s'engage à faciliter la reprise de son poste de travail en cas d'absence quel qu'en soit le motif.

**Article III. Principes de sécurité**

**Section 3.01 Règles de sécurité applicables**

L'université de Toulouse II – Le Mirail met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les codes d'accès 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 codes d'accès ;
- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

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

✓ de la part de l'institution :

- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service 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 :

- s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'institution, ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou l'établissement ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'institution, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de sa hiérarchie ;
- se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques ;
- ne pas interrompre le fonctionnement normal du réseau ou des systèmes connectés ;
- ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, saturer les ressources ;
- ne pas introduire des programmes malveillants ou contournant la protection des logiciels ;
- ne pas s'attaquer aux systèmes d'information de l'UTM ou de tout autre organisme public ou privé, européen ou étranger, en modifier ou altérer le contenu ;
- ne pas collecter ou tenter de collecter des informations susceptibles d'être utilisées lors de tentatives d'attaques contre des systèmes d'information externes ou internes ;
- ne pas utiliser les ressources informatiques afin de dupliquer, diffuser ou distribuer des logiciels, images, sons et vidéos aux contenus visés par le code pénal ou collectés par des moyens contraires au

droit de la propriété intellectuelle, sous quelque forme que ce soit.

**Section 3.02 Devoirs de signalement et d'information**

L'utilisateur doit avertir sa hiérarchie et la Direction du Système d'Information 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 correspond pas à son habilitation.

**Section 3.03 Mesures de contrôle de la sécurité**

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'institution 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 de 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 de Toulouse II – Le Mirail informe l'utilisateur que le système d'information donne lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur.

En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou si elles tombent dans le champ de l'article[7] 40 alinéa 2 du code de procédure pénale.

**Article IV. Communication électronique**

**Section 4.01 Messagerie électronique**

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

**(a) Adresses électroniques**

L'institution s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative[8] lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'utilisateur.

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.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'institution.

**(b) Contenu des messages électroniques**

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son

[7] Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.
[8] Par exemple, l'adresse est de la forme prénom.nom@ac-<nom de l'académie>.fr ou prénom.nom@<nom de domaine institutionnel>.fr

caractère privé[9] ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur par le fournisseur de service de messagerie.

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 (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques...).

**(c) Émission 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.

**(d) 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[10] 1369-1 à 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.

**(e) 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.

**(f) Listes de diffusion**

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'institution : ces listes ne peuvent être utilisées sans autorisation explicite.

Sous réserve de ne pas porter atteinte au droit à l'expression syndicale, l'utilisation de listes de diffusion à des fins non professionnelles est prohibée et est susceptible d'entrainer l'engagement de la responsabilité pénale et/ou disciplinaire de l'auteur.

**Section 4.02 Internet**

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension 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'institution.

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques). Si une utilisation résiduelle privée, telle que définie en section 2.01, peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'administration sont présumées avoir un caractère professionnel. L'administration peut les rechercher aux fins de les identifier.

**(a) Publication sur les sites internet et extranet de l'institution**

Les agents étant appelés à publier des informations via les dispositifs numériques de l'université sont informés que leurs publications pourront faire l'objet d'un contrôle a posteriori par l'institution.

Aucune publication de pages d'information à caractère privé (pages privées ...) sur les ressources du système d'information de l'institution n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le service ou l'établissement.

---

[9] Pour exemple, les messages comportant les termes ("privé") dans l'objet ou sujet du message

[10] Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne

**(b) Sécurité**

L'université de Toulouse II – Le Mirail 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.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou l'établissement.

L'université de Toulouse II Le-Mirail se réserve le droit de filtrer ou d'interdire l'usage d'applications ou l'accès à des services en ligne lorsqu'ils sont susceptibles d'engendrer des dysfonctionnements internes ou ouvrent une ou des failles de sécurité reconnue(s).

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formations ou de campagnes de sensibilisation.

### Section 4.03 Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article VI.

L'institution 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, codes malveillants, programmes espions ...).

## Article V. Traçabilité

L'université de Toulouse II - Le Mirail est dans l'obligation légale de mettre en place un système de journalisation[11] des accès Internet, de la messagerie et des données échangées.

L'université de Toulouse II - Le Mirail se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes d'information.

Préalablement à cette mise en place, l'institution procèdera, auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL), à une déclaration, qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n° 78-17 du 6 janvier 1978 modifiée.

## Article VI. Respect de la propriété intellectuelle

L'institution rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, 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.

## Article VII. 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 à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite «Informatique et Libertés» modifiée.

Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit -

[11] Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur

directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi «Informatique et Libertés».

En conséquence et dans l'attente de la désignation d'un Correspondant Informatique et Liberté (CIL[12]) de l'UTM, tout utilisateur souhaitant procéder à une telle création devra informer les services de l'université compétents (affaires juridiques et DSI) qui prendront les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de cette loi, 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 du responsable hiérarchique du service ou de l'établissement dont il dépend.

**Article VIII. Limitation des usages**

En cas de non-respect des règles définies dans la présente charte, pourront, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, être limité les usages par mesure conservatoire.

**Supprimé :** il

**Supprimé :** a

Par «personne juridiquement responsable», il faut entendre toute personne ayant la capacité de représenter l'institution (ministre, directeur, recteur, inspecteur d'académie, chef d'établissement...).

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est passible de sanctions. L'université ne pourra être tenu pour responsable de l'usage frauduleux par les usagers des outils mis à leur disposition.

**Article IX. Entrée en vigueur de la charte**

Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des systèmes d'information pour les personnels et assimilés.

**Le président de l'Université de Toulouse II – Le Mirail,**

[12] Au sein de l'Université, le CIL est un vecteur de diffusion de la réglementation en matière de protection des données à caractère personnel et de la culture « Informatique et Liberté ». Il est un interlocuteur entre la présidence, les instances de décisions, les unités pédagogiques, les laboratoires de recherches, les usagers de l'université et la CNIL. Vous retrouverez dans la « Fiche n°4 Correspondant Informatique et Libertés » du Guide 'Informatique et Libertés' pour l'enseignement supérieur et la recherche », une description précise de son rôle et de ses missions (ce guide est en ligne sur les sites de la CPU, de l'AMUE et de la CNIL).