

La charte pour l'utilisation des ressources informatiques de l'UTT (ci-après « la charte ») a pour objet de définir les conditions d'accès au système d'information de l'UTT et aux ressources informatiques par la description des droits et devoirs des utilisateurs dans le respect de la législation française et internationale.

I. DOMAINE D'APPLICATION DE LA CHARTE

La charte définit une politique générale que doit respecter tout utilisateur s'il veut pouvoir accéder :

- au parc informatique de l'UTT (postes de travail et logiciels),
- au réseau informatique de l'UTT (réseau local et réseau internet) depuis un équipement informatique (poste de travail, smartphone, tablettes ...) personnel ou non,
- au système d'information de l'UTT.

Sont entendues comme utilisateurs du système d'information et des ressources informatiques de l'UTT les personnes suivantes :

- étudiants ;
- enseignants, chercheurs, enseignants-chercheurs, chargés d'enseignement vacataires, chercheurs associés ;
- personnels administratifs et techniques ;
- personnes accueillies temporairement (stagiaires, invités, intervenants extérieurs...);
- association hébergées à l'UTT.

II. PRINCIPES GÉNÉRAUX

1. Respect des règles éthiques

Sont strictement prohibées les utilisations contraires aux lois et règlements en vigueur et notamment celles qui ont pour objet ou pour effet, la diffusion d'idéologies xénophobes, antisémites ou raciste.

Les utilisateurs s'interdisent toute diffamation, injure publique ou propos condamnables.

2. Respect de la vie privée

Conformément à l'article 9 du code civil « chacun a droit au respect de sa vie privée. A ce titre, aucune image ou information relative à la vie privée d'autrui ne peut être mise en ligne sans le consentement de la personne intéressée.

3. Constitution de fichiers contenant des informations nominatives

Pour la création de fichiers contenant des informations nominatives, les utilisateurs et administrateurs de l'UTT s'engagent à respecter les dispositions de la loi informatique et liberté, qui prévoit une obligation de déclaration de constitution de fichiers contenant des informations nominatives à la Commission Nationale de l'Informatique et des Libertés (CNIL) conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Pour effectuer leurs démarches, les utilisateurs peuvent se renseigner auprès du Correspondant Informatique et Liberté de l'établissement, en lui écrivant par mail à l'adresse : cil@utt.fr

4. Filtrage

L'UTT se réserve le droit de filtrer ou d'interdire l'accès à certaines catégories de sites illégaux ou présentant une menace avérée pour la sécurité de son système d'information, après information du C.Tp. La liste de ces catégories de sites est diffusée aux utilisateurs.

5. Politique de gestion des journaux informatiques

L'UTT a mis en place une politique de gestion des journaux informatiques (détaillée en annexe de la présente charte) sur tous les outils et services numériques qu'elle met à la disposition des utilisateurs.

Les utilisateurs sont informés que la durée légale de conservation des fichiers de journalisation est d'une année à partir de la date d'enregistrement. L'UTT s'interdit de les exploiter au-delà de 3 mois sauf sur réquisition de justice ou sous une forme rendue anonyme.

6. Propriété intellectuelle

L'UTT rappelle que l'utilisation des moyens numériques implique le respect de ses droits de propriété intellectuelle notamment les droits d'auteur ainsi que ceux de ses partenaires et, plus généralement, de tous tiers titulaires de tels droits. En conséquence, chaque utilisateur doit notamment s'abstenir de reproduire, copier tout contenu sans autorisation préalable du ou des titulaires de ces droits.

7. Usage professionnel

Les moyens numériques et matériels mis à disposition des utilisateurs par l'UTT le sont dans le cadre d'un usage professionnel. Au sens de la présente charte, l'usage de ces moyens présente un caractère professionnel lorsqu'il intervient :

- dans le cadre des missions confiées par l'UTT, pour les utilisateurs membres de son personnel : enseignants, personnels administratifs ou techniques, mais également ses prestataires et partenaires ;
- dans le cadre des activités pédagogiques, pour ses utilisateurs étudiants.

Par conséquent, l'utilisation à des fins privées doit être non lucrative et limitée. Elle ne doit nuire ni à la qualité du travail de l'utilisateur, ni au temps qu'il y consacre, ni au bon fonctionnement du service.

8. Respect des règles de déontologie informatique

Il est interdit de :

- de masquer sa véritable identité ;
- de s'approprier le mot de passe d'un autre utilisateur ;
- d'altérer, de modifier des données et 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 système connecté au réseau ;
- d'installer des programmes destinés à intercepter des trames émises sur le réseau à destination d'autres personnes sans en informer le responsable de la sécurité du système d'information (RSSI). Trouver de tels programmes sur une machine en dehors d'un programme de recherche ou d'enseignement reconnu par le RSSI indique pour le moins une tentative d'action illégale, répréhensible ;
- 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 ;
- de dégrader le matériel de l'UTT ;
- d'utiliser sur le réseau de l'université des moyens de cryptologie qui ne respectent pas la réglementation relative à la cryptologie ;

III. DROITS ET DEVOIRS DES UTILISATEURS

1. Accès

Chaque utilisateur se voit attribuer un code d'accès (un identifiant et un mot de passe) pour la durée de ses fonctions au sein de l'UTT ou pour la durée de sa scolarité s'il est étudiant. **Ces codes d'accès sont strictement personnels et incessibles.**

Les mots de passe doivent être changés régulièrement et ne doivent correspondre ni à un mot courant ni à un nom propre dans quelque langue que ce soit.

Les accès prennent en compte les besoins particuliers de chaque utilisateur et peuvent évoluer en fonction de variations dans la situation de l'utilisateur.

Dans le cas des étudiants, et pour certaines UV, ils se voient pourvus de comptes génériques de TP (pour la durée de leur inscription à l'UV) également protégés par un mot de passe, ces comptes doivent obéir aux mêmes règles que tout autre compte utilisateur.

En cas de problèmes sur son compte d'accès (usurpation d'identité, difficultés d'accès), l'utilisateur s'engage à prévenir le CRI dans les meilleurs délais.

2. Raccordement au réseau de l'UTT

L'utilisation d'un logiciel anti-virus (avec des définitions de virus à jour) est obligatoire lors de la connexion de tout poste informatique filaire ou Wifi au réseau de l'UTT.

3. Messagerie électronique de l'UTT

a) Caractère professionnel

Tout échange via la messagerie électronique est réputé professionnel à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace prévu à cet effet et identifié sans ambiguïté comme tel. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

b) Gestion des courriels

La gestion des courriels électroniques à l'intérieur de la boîte aux lettres (archivage, suppression) revient à l'utilisateur.

La capacité de stockage de la boîte aux lettres étant limitée pour les étudiants, une fois le quota presque atteint, un mail automatique d'information lui est envoyé, il doit alors réagir sans plus attendre. Sans réaction de sa part ses nouveaux mails seront perdus et l'utilisateur devra se présenter au CRI pour réactiver sa boîte.

La disponibilité de la messagerie de l'utilisateur est garantie hors cas de réalisation de diagnostic et de maintenance par les administrateurs sur le réseau ou de force majeure.

c) Devoir particulier concernant l'envoi de courriels

Les utilisateurs s'engagent à ne transmettre les messages et documents qu'aux seules personnes auxquelles ils sont destinés et à cibler les contacts de leurs listes de diffusion.

4. Utilisation des matériels de l'UTT

a) Principe du droit à l'intégrité et à la confidentialité des fichiers (comptes Windows, Unix ...)

L'administrateur système s'engage à respecter l'intégrité et la confidentialité des fichiers sur les différents comptes de l'utilisateur. Cependant dans la limite de la réalisation de diagnostic ou de correction de problèmes sur ce dernier ou sur le système d'information de l'UTT, il sera possible à l'administrateur d'accéder aux fichiers.

Si l'utilisateur le désire, il peut apposer sur le fichier ou dossier de son compte la mention "privé" ou « personnel ». L'administrateur n'ouvrira ce type de dossier qu'en présence de l'utilisateur ou sur demande ou autorisation judiciaire. . En cas d'échec de décontamination d'un fichier par le logiciel anti-virus de l'université, le fichier sera détruit.

b) Principe du droit à la disponibilité des comptes et services sur le système d'information de l'UTT

La disponibilité des fichiers, dossiers, travaux de l'utilisateur est garantie hors cas de réalisation de diagnostic, de maintenance par les administrateurs sur le réseau ou de force majeure.

La disponibilité des fichiers est limitée dans le temps ou en raison de conditions spécifiques.

L'utilisateur reconnaît que l'ensemble de ses fichiers ne lui seront plus accessibles à la date d'expiration de ses droits sur le système d'information de l'UTT.

L'utilisateur privé de ses droits en raison de la violation des dispositions de la charte perd automatiquement son accès au système d'information de l'UTT et à l'ensemble de ses fichiers, dossiers...

c) Bonne utilisation

L'ensemble des utilisateurs s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition et notamment s'engage à avertir le CRI de tout problème (erreur logicielle, vol de matériel...).

La taille de l'espace disque disponible pour chaque compte étant limitée, l'utilisateur doit respecter la taille de l'espace disque qui lui est alloué et utiliser les outils de compression de fichier qui sont mis à sa disposition.

Il doit être fait un usage raisonnable de toutes les ressources informatiques partagées afin de maintenir une puissance de calcul, un espace disque, une bande passante sur le réseau de l'université, optimaux. Une durée d'occupation des postes de travail en libre service conforme aux souhaits individuels et collectifs doit être observée. En outre, les actions légales s'inscrivant dans les activités de l'université risquant d'accaparer fortement les ressources informatiques devront être effectuées aux moments qui pénalisent le moins la communauté.

d) Installation de logiciels

Il n'est pas permis :

- d'utiliser des logiciels dits de « peer-to-peer » ou ceux clairement prohibés sur le réseau de l'UTT dont la liste est présentée, pour information au CTP et diffusée aux utilisateurs ;
- de faire une copie d'un logiciel non libre de droits ;

(NB : La constitution de copies de sauvegarde est un droit appartenant à l'administrateur) ;

- de contourner les restrictions d'utilisation d'un logiciel ;
- de développer des programmes constituant ou pouvant s'apparenter à des virus.

Il est fortement déconseillé d'installer des logiciels sans passer par le CRI. Lorsqu'un utilisateur installe un logiciel sans l'accord du CRI il s'engage, de ce fait, à en assumer les responsabilités techniques et juridiques.

L'UTT a déployé une protection logicielle généralisée non seulement sur les serveurs mais aussi sur les postes de travail lui appartenant.

Sur chaque poste utilisateur est installé un anti-virus. Il est interdit par la présente charte de désactiver, d'altérer le fonctionnement ou de désinstaller ce client. Il est aussi interdit d'utiliser d'autres logiciels (anti-virus ou autres) susceptibles d'entraîner un dysfonctionnement de l'anti-virus installé en exécution de la stratégie de sécurité de l'UTT.

Lorsqu'un utilisateur installe un logiciel sans être passé par le CRI, il s'engage à en assumer les responsabilités techniques et juridiques.

L'utilisateur doit prendre conscience de l'impact du téléchargement de logiciel, sur la bande passante de l'UTT et des risques qu'il fait courir à l'intégrité du système d'information puisque ces logiciels peuvent être contaminés par des chevaux de Troie et des virus.

L'utilisateur doit avoir installé un anti-virus avant de pouvoir raccorder son poste personnel au réseau wifi de l'UTT.

e) Utilisation des logiciels et bases de données numériques

Pour chacun des logiciels et bases de données numériques, des droits d'utilisation sont accordés à l'UTT. Ils doivent être utilisés conformément à leur destination. Leur utilisation ne peut dépasser le cadre de l'activité de l'utilisateur à l'UTT. Ainsi, toute utilisation à des fins lucratives et/ou privés est prohibée.

Concernant l'enseignement, l'ensemble des logiciels disponibles sur le système d'information est détaillé sous forme de liste qui est affichée dans les différentes salles informatiques et sur l'ENT.

5. Sites web, E-portfolio et pages personnelles

Lors de la création de sites ou pages qui seront à terme :

- hébergés sur les serveurs de l'UTT ;
- ou ayant un lien direct avec l'université ;

les utilisateurs s'engagent à déclarer le thème général du site auprès du CRI et du service communication. Ce thème doit être en conformité avec les objectifs poursuivis par l'université.

En utilisant le système de E-portfolio de l'UTT, les utilisateurs acceptent les conditions d'utilisation ainsi que les règles concernant la protection des données à caractère personnel.

Les pages publiées à l'intention d'un groupe d'utilisateurs, de tous les utilisateurs, ou du public, doivent respecter les règles de la communication publique, et sont publiées sous la seule responsabilité de leurs auteurs.

Les utilisateurs s'interdisent toute diffamation, injure publique ou propos condamnables. Tout manquement à cette règle doit être signalé aux administrateurs qui ont la possibilité d'interrompre la diffusion des pages concernées et de suspendre à titre conservatoire le compte des utilisateurs, sans présumer des poursuites éventuelles devant les instances disciplinaires de l'Université.

Les pages montrées à un seul utilisateur ou celles montrées par le mécanisme de l'URL secrète, sont soumises aux règles de la communication privée et sont en particulier protégées par le secret des correspondances. Leur destinataire s'interdit donc de les montrer à des tiers et s'engage à en garantir la confidentialité.

L'université n'est pas responsable juridiquement des contenus mis en ligne sur les sites définis ci-dessus, les contenus sont mis en ligne sous la responsabilité de ceux qui les publient.

6. Trombinoscope

Un trombinoscope est établi pour certaines formations de l'Université de Technologie de Troyes. Le trombinoscope traite des données nominatives : noms, prénoms, formation, il fait l'objet d'une déclaration spéciale par l'UTT à la Commission Nationale de l'Informatique et des Libertés conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

L'utilisateur peut refuser de figurer dans le trombinoscope, pour cela il peut le préciser au moment de la prise de photo.

IV. LES ADMINISTRATEURS

Les administrateurs sont toutes les personnes qui interviennent sur un ou plusieurs éléments d'une ressource informatique :

- les postes de travail individuels ;
- les bases de données ;
- les serveurs ;
- le réseau ;
- les applications (serveur/client) ;
- la téléphonie.

Ils assurent le bon fonctionnement général du système d'information.

Ils ont un devoir d'information vis-à-vis des utilisateurs et sont tenus au respect de la confidentialité des informations qu'ils peuvent détenir.

Les administrateurs peuvent être amenés à interrompre le fonctionnement du réseau, complet ou partiel à des fins de maintenance. Les utilisateurs en seront préalablement informés.

L'utilisation des différents services génère des fichiers de traces (journaux informatiques) qui sont conservés à des fins d'identification des utilisateurs en cas d'infraction. Ainsi en cas de tentative de piratage d'un réseau privé via le système d'information de l'UTT, l'administrateur doit être en mesure de fournir l'identité de la personne grâce aux logs de connexion, en respectant le principe de confidentialité et les dispositions énumérées ci-dessus.

V. Conséquences au manquement à la charte

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

VI. Principaux textes juridiques de référence

- Loi n° 2004-575 du 21 Juin 2004 pour la confiance dans l'économie numérique
- Art. 323-1 à 323-7 du Code Pénal relatifs à la fraude informatique.
- Loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- Art. 226-16 à 226-23 du Code Pénal: atteintes au droit de la personne résultant des fichiers ou des traitements informatiques;
- Art. 226-24 du Code Pénal instituant la responsabilité pénale des personnes morales pour ces mêmes infractions (art. 226-16 à 23).
- Art. 335-2-1 et 335-3 du code de la propriété intellectuelle sur la protection des logiciels.
- Art. 226-15 et 432-9 et du Code Pénal secrets des correspondances (écrites, transmises par voie de télécommunications).
- Le code de la propriété intellectuelle.

Cette liste n'est pas exhaustive.

L'utilisateur et les administrateurs reconnaissent pouvoir encourir des sanctions disciplinaires, civiles et pénales, en cas de non-respect de la charte.