UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

Charte des usages numériques

Préambule

La présente Charte a pour objet de fixer les règles d'usage des moyens numériques de l'Université de Paris 1 Panthéon-Sorbonne.

Cette Charte a pour objet d'informer les utilisateurs de leurs droits et de leurs responsabilités à l'occasion de l'usage des ressources informatiques et des services numériques de l'Université, en accord avec la législation.
Elle répond également à la préoccupation de l'Université de protéger les informations qui constituent son patrimoine immatériel contre toute altération, volontaire ou accidentelle, de leur confidentialité, intégrité ou disponibilité.

Elle permet, par l'observation par chacun des principes et des règles énoncés ci-après, de garantir la sécurité du système d'information, la disponibilité maximum des outils numériques, pour l'ensemble des utilisateurs de l'Université.

Cette Charte, annexée au règlement intérieur, s'applique à chaque utilisateur. Elle vise à assurer un usage correct des ressources numériques et des services proposés, avec des règles minimales de courtoisie et de respect d'autrui.

Sommaire

Préambule 1

Sommaire 2

1 Définitions 3

2 Accès au réseau de l'Université - Bornes Wi-Fi 3
- 2.1 Caractère professionnel de l'accès 3
- 2.2 Accès internet 4
- 2.3 Sécurité 4
- 2.4 Autres matériels connectés 5

3 Ouverture d'un compte utilisateur – Accès aux applications 5
- 3.1 Respect des droits d'accès 6
- 3.2 Protection des mots de passe et des droits d'accès 6
- 3.3 Confidentialité des informations 7

4 Courriels et messagerie 8
- 4.1 Mise à disposition d'une adresse mail 8
- 4.2 Contenu des échanges par courriel 9
- 4.3 Bonnes pratiques – Droit à la déconnexion 10

5 Postes de travail 11
- 5.1 Postes en libre-service 11
- 5.2 Autres postes de travail 11
- 5.3 Utilisation privée d'un poste de travail 14
- 5.4 Utilisation du poste en mode administrateur 14
- 5.5 Connexion d'un matériel personnel au réseau 15
- 5.6 Télétravail 15
- 5.7 Téléphone 15

6 Informatique et libertés 16
- 6.1 Droits d'accès 16
- 6.2 Créations de fichiers nominatifs 16
- 6.3 Mesures de garantie du bon fonctionnement et contrôle de la sécurité 16

7 Rappel de la législation applicable 17

8 Divers 18
- 8.1 Applicabilité 18
- 8.2 Entrée en vigueur de la Charte 18
- 8.3 Limitations et sanctions applicables 19
- 8.4 Autres chartes 19
- 8.5 Aide-mémoire des droits et obligations 20

1 Définitions

Les *utilisateurs* au sens de la présente Charte, sont définis comme l'ensemble des personnes ayant l'autorisation d'accéder au réseau, aux ressources informatiques ou au système d'information de l'Université, quel que soient leurs statuts (personnels administratifs, enseignants, étudiants, alumni, lecteurs des bibliothèques, etc.).L'écriture inclusive n'a pas été utilisée pour la présente Charte pour offrir une meilleure lisibilité.

L'*Université* désigne dans la présente charte l'Université de Paris 1 Panthéon-Sorbonne, l'ensemble de ses composantes ou de ses services, ou de ses partenaires telles que les unités de recherche, dès lors qu'ils accèdent au réseau informatique de l'Université ou qu'ils sont hébergés dans ses locaux.

Les usages numériques recouvrent toute utilisation des moyens informatiques de traitement de l'information, tels que le réseau de l'Université (incluant l'accès Wi-Fi), les applications, les outils et services mis à la disposition des utilisateurs (incluant l'accès à Internet). Ces ressources informatiques, constituées de matériels, de logiciels et de données constituent le système d'information de l'Université. Elles peuvent être accessibles depuis les locaux de l'Université ou à distance.

Le *service informatique* désigne les équipes (en général de la DSIUN, la Direction des Systèmes d'Information et des Usages Numériques) en charge du support de proximité.

2 Accès au réseau de l'Université - Bornes Wi-Fi

L'Université offre à ses utilisateurs un accès à son réseau.
Cet accès peut se faire sous la forme d'un raccordement filaire à une prise murale, ou être un accès sans fil de type Wi-Fi.

2.1 Caractère professionnel de l'accès

L'utilisation du réseau de l'Université, permettant l'accès à internet ou aux ressources informatiques de l'Université est autorisée dans le cadre de l'*activité professionnelle des personnels et de travaux des utilisateurs liés aux enseignements dispensés à l'Université, à son patrimoine documentaire ou à toute action de diffusion des savoirs qu'elle conduit. Le terme « professionnel » sera utilisé dans ce document pour caractériser ce type d'activités.*

Ces conditions sont celles prévues par les statuts du *GIP RENATER* auquel est liée l'Université, à savoir : *les activités de recherche, d'enseignement, de développements techniques, de transfert de technologie, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentation de nouveaux services présentant un caractère d'innovation technique, mais également toute activité administrative et de gestion découlant ou accompagnant ces activités.*

Si une utilisation ponctuelle à titre privé peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'Université sont présumées avoir un caractère professionnel.

L'utilisation des ressources réseau doit être rationnelle et loyale, afin d'éviter leur saturation ou leur détournement à des fins personnelles. L'utilisateur doit appliquer les recommandations de sécurité et de bon usage des moyens auxquels il a accès. L'usage privé de l'accès à internet ne doit pas par exemple apporter de perturbations au bon fonctionnement du réseau de l'Université.

2.2 Accès internet

L'Université met à la disposition de l'utilisateur un accès à internet chaque fois que cela est possible.

Respect de la législation

Il est rappelé que le réseau internet est soumis à l'ensemble des règles de droit en vigueur. La législation concernée est rappelée au chapitre 7.
Tout téléchargement de fichiers, notamment de sons ou d'images, doit s'effectuer dans le respect des droits de propriété intellectuelle.
La consultation volontaire ou répétée de sites répréhensibles ou non appropriés (par exemple des sites pornographiques) depuis le réseau de l'Université est proscrite.

Journalisation des accès

L'Université, dans la mesure où elle fournit un accès à internet, est dans l'obligation légale de mettre en place un système de journalisation des accès à son réseau.
Les dispositifs de protection des données personnelles ainsi recueillies sont décrits au paragraphe 6.3.

Responsabilité de bon fonctionnement

L'Université maintient son réseau et l'accès à internet dans un état de bon fonctionnement.
Pour garantir la qualité de la connexion ou en cas de dysfonctionnement, l'Université peut :

- filtrer ou interdire l'accès à certains sites ;
- limiter le téléchargement de certains fichiers trop volumineux ;
- bloquer le téléchargement de fichiers présentant un risque pour la sécurité des systèmes d'information, tels les virus, code malveillant ou programmes espions ;
- procéder à des statistiques anonymisées mesurant le trafic, incluant les sites visités ou les durées de connexions.

2.3 Sécurité

Responsabilité individuelle

Par sa vigilance et par le respect des règles de sécurité, l'utilisateur contribue à la sécurité générale de l'Université.
L'utilisateur est en effet le premier acteur de la sécurité : on estime que plus de 95 % des infections de virus ou de codes malveillants proviennent d'une action utilisateur ; ouverture d'un mail piégé, introduction d'une clé USB compromise, téléchargement d'un logiciel ou visite d'un site web malveillant.
Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auquel il a accès et contribue à la sécurité de l'Université, de sa composante ou de son service. A son niveau, le personnel d'encadrement favorise l'instauration d'une « culture sécurité » par son exemplarité dans le respect de cette Charte et par un soutien actif des équipes en charge de la mise en œuvre de ces règles.

Sécurité sur internet

Des risques liés à la sécurité sont présents sur internet comme par exemple :

- des sites malveillants qui profitent des failles des navigateurs pour récupérer les données présentes sur le poste de travail ;
- la mise à disposition de logiciels qui, sous une apparence anodine, peuvent prendre le contrôle de l'ordinateur et transmettre son contenu au pirate à l'insu de l'utilisateur ;
- l'utilisation abusive des données transmises ou saisies.

D'autres risques sont liés à des mails piégés (hameçonnage ou *phishing*) et aux pièces jointes ou aux liens qu'ils contiennent. Ils seront détaillés au paragraphe 4.3.
Par conséquent, l'utilisateur :

- évite de se connecter à des sites qui lui paraissent suspects ;
- prête une attention particulière à l'origine des logiciels qu'il télécharge ;
- se tient informé des bonnes pratiques de sécurité informatique telles que préconisées par les pouvoirs publics notamment.

L'Université conduit régulièrement des campagnes de sensibilisation ou des actions de formations informant l'utilisateur des risques et limites inhérents à l'utilisation d'internet, et veille à donner les conseils de sécurité appropriés.

Respect des règles de sécurité

L'utilisateur :

- s'engage à ne pas apporter volontairement de perturbations au bon fonctionnement des ressources informatiques et des réseaux, par des manipulations anormales du matériel ou des logiciels ;
- n'installe pas, ne télécharge pas ou n'utilise pas sur les matériels connectés des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou provenant de sites douteux ou signalés comme tels ;
- s'engage à ne jamais introduire volontairement sur le réseau de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques, malwares, spywares, ...
- reste vigilant vis-à-vis des supports de données amovibles (clé USB, disque externe, DVD, etc.) introduits sur des matériels connectés et prend les précautions nécessaires pour s'assurer de leur innocuité ;

L'accès à internet n'est autorisé qu'au travers des dispositifs mis en place par l'Université. Il est interdit de connecter au réseau de l'Université des bornes Wi-Fi, des box d'accès à internet ou des ordinateurs équipés d'une clé 3G/4G/5G en activité, qui créeraient ainsi une interconnexion non maîtrisée avec internet.

Besoins spécifiques

Si un service, une composante ou un chercheur de l'Université, dans le cadre de ses travaux, a des besoins spécifiques dérogeant aux règles ci-dessus ou exprime le besoin d'outrepasser les règles de sécurité et les contrôles mis en place, il doit s'adresser au service informatique qui définira avec lui une solution adaptée.

2.4 Autres matériels connectés

Devant le développement rapide de nouveaux dispositifs connectés, il est rappelé que les règles ci-dessus concernent tout type de matériel dès lors qu'il se connecte au réseau de l'Université, en filaire ou via une connexion sans fil : ordinateur fixe, ordinateur portable, tablette, smartphone, montre connectée ou plus généralement tout objet connecté.
Le caractère présumé professionnel de l'accès, le respect du bon fonctionnement du réseau, de sécurité, ou la possibilité d'enregistrement des journaux de connexions s'appliquent potentiellement à tout type de matériel dès lors qu'il utilise les services réseaux de l'Université.

3 Ouverture d'un compte utilisateur - Accès aux applications

L'Université offre à ses utilisateurs l'accès à des services ou à des applications.

Pour mettre en œuvre les mécanismes de protection appropriés, l'Université attribue un compte à chacun et met à la disposition des utilisateurs différents dispositifs d'authentifications tels que des mots de passe, des badges ou des certificats.
L'Université met en œuvre différents moyens permettant de protéger la sécurité de l'utilisateur et la confidentialité de ses informations. L'utilisateur doit respecter les consignes de sécurité telles que les règles relatives à la gestion des mots de passe.

3.1 Respect des droits d'accès

Caractère individuel des droits d'accès

L'utilisateur doit respecter les droits d'accès qui lui ont été attribués :

- ces autorisations sont strictement personnelles : il ne doit pas les céder, même temporairement à un tiers ;
- il respecte la gestion des accès, il ne cherche pas à connaître les mots de passe d'autres personnes ni à faire usage des droits d'accès d'une tierce personne ;
- il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers ;
- de la même façon, il n'essaie pas de masquer sa propre identité.

En tout état de cause, l'utilisateur est responsable de l'utilisation des systèmes d'information réalisée avec ses droits d'accès.

Lien entre droits d'accès et missions confiées

Les niveaux d'accès ouverts aux utilisateurs sont définis en fonction de son rôle ou de la mission qui lui est confiée.
Toute autorisation prend fin lors de la cessation, même provisoire de l'activité professionnelle ou d'études qui l'a générée. En complément des procédures prévues liées à l'arrivée et au départ, l'utilisateur s'assure que ses droits ont été mis à jour et informe si nécessaire les administrateurs du service informatique de toute évolution de ses fonctions nécessitant une modification de ses droits d'accès.
Des statuts spécifiques d'utilisateurs peuvent être attribués aux anciens étudiants (alumni) ou aux anciens agents de l'Université (retraités, enseignants émérites), pendant une période définie, pour maintenir certains droits d'accès, tels que l'accès à la messagerie.

Respect des limitations

L'utilisateur autorisé doit se connecter sur un serveur via les procédures qui lui ont été communiquées et ne doit pas essayer de les contourner ou de se connecter sans y être autorisé par les responsables habilités.
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.
Il signale immédiatement au service informatique toute faille de sécurité ou toute possibilité d'accès non contrôlé qu'il découvre.
Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède, par exemple en tentant de tester leur sécurité.

3.2 Protection des mots de passe et des droits d'accès

Mots de passe

L'utilisateur choisit des mots de passe sûrs :

- Il applique les règles de complexité de mot de passe et de renouvellement en vigueur ;

- Il utilise des mots de passe distincts pour ses usages professionnels et ses usages privés ;
- Il garde strictement confidentiels son ou ses mots de passe ;
- Il ne les communique jamais, y compris à son responsable hiérarchique et au service informatique.

Protection des moyens

L'utilisateur assure la protection des moyens d'authentification qui lui ont été affectés ou qu'il a générés (badges, mots de passe, clés privées, etc.) :

- Il met en place tous les moyens mis à sa disposition pour éviter la divulgation de ses moyens d'authentification ;
- Il modifie ou demande le renouvellement de ses moyens d'authentification dès lors qu'il en suspecte la divulgation ;
- Il doit signaler toute tentative de violation de son compte, et, de façon générale toute anomalie ou utilisation illicite qu'il peut constater ;
- L'utilisateur doit avertir le service informatique dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information.

3.3 Confidentialité des informations

Protection des informations

L'utilisateur protège les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité.
Lorsqu'il crée un document, l'utilisateur détermine son niveau de sensibilité et applique les règles permettant de garantir sa protection durant tout son cycle de vie (marquage, stockage, transmission, impression, suppression, etc.).
Afin de se prémunir contre les risques de vol de documents sensibles, l'utilisateur, lorsqu'il s'absente de son bureau, s'assure que ses documents papier, lorsqu'ils existent, sont rangés sous clé et que son poste de travail est verrouillé.

Il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement ni en copie.
De même, l'utilisateur ne recopie pas ou ne diffuse pas des ressources pédagogiques non publiques, qui ne doivent rester accessibles qu'aux étudiants concernés.

Publication d'informations sur internet

L'utilisateur veille à ne pas publier sur internet d'informations sensibles ou confidentielles. Il n'utilise pas internet pour effectuer des sauvegardes des données de son poste. Il utilise si nécessaire un système de chiffrement pour garder confidentiel une information stockée dans un espace accessible sur internet. Il veille à utiliser des sites et des applications de confiance, et suit les recommandations éventuelles données par son service informatique.

L'utilisateur utilise ses coordonnées professionnelles, en particulier son adresse électronique ou autre identifiant, avec précaution. En les utilisant de façon inappropriée, il facilite les atteintes à sa réputation et à la réputation de l'Université ; l'Université se réserve le droit d'agir en justice à son encontre pour protéger son image.
L'utilisateur utilise ses coordonnées personnelles pour les sites sans rapport avec son activité professionnelle.

Toute publication d'information sur les sites internet ou intranet de l'Université est réalisée sous la responsabilité d'un responsable de site ou responsable de publication nommément désigné.
La publication d'information à caractère privé (pages privées au sens non professionnelles) sur les ressources du système d'information de l'Université n'est pas autorisée.

Réseaux sociaux

Les réseaux sociaux permettent aujourd'hui une grande liberté d'expression. Ils peuvent par mégarde exposer au vu de tous des informations au départ destinées à un cercle restreint.
Au-delà d'une utilisation privée, les pages sur les réseaux sociaux qui se réclament de l'Université doivent faire l'objet d'une communication maîtrisée. L'Université reste garante en dernier ressort de la qualité éditoriale et de l'exactitude des contenus présents. Ces pages ne doivent être publiées que par des personnes habilitées (comme indiqué dans la « Charte du Web et des réseaux sociaux » de l'Université).

4 Courriels et messagerie

L'Université s'engage à mettre à la disposition de l'utilisateur une adresse mail lui permettant d'émettre et de recevoir des messages électroniques sur une boîte à lettres nominative.
De bonnes pratiques d'utilisation de la messagerie, incluant notamment un « droit à la déconnexion » sont présentées ci-après et détaillées dans le « Guide des bonnes pratiques de la messagerie ».

4.1 Mise à disposition d'une adresse mail

Caractère professionnel

La messagerie est un outil de travail destiné à des usages professionnels. L'utilisation de cette adresse nominative se fait sous la responsabilité de l'utilisateur ; elle engage aussi l'Université.
Pour le personnel administratif, l'adresse professionnelle doit être utilisée systématiquement pour les usages professionnels, et l'utilisation d'une adresse personnelle est à proscrire. Pour le personnel enseignant, il est recommandé d'utiliser l'adresse professionnelle.

Messages à caractère privé

Un usage privé de la messagerie peut être toléré de façon ponctuelle, dès lors qu'il n'apporte pas de perturbation au bon fonctionnement de la messagerie de l'Université.
Tout message sera considéré comme professionnel sauf s'il comporte en objet la mention "privé" ou « personnel » ou s'il est stocké dans un espace spécifique de données identifié comme tel.

Sécurité

L'utilisateur doit respecter les règles de sécurité régissant l'accès à sa boîte mail, telles que la fourniture d'un mot de passe ou la limitation du type d'appareil autorisé à accéder à sa boîte mail.

Archivage des messages électroniques

Les mesures de conservation des données professionnelles, notamment pour garantir la continuité de service, sont définies avec le responsable hiérarchique.
Chaque utilisateur doit organiser et assurer la conservation des messages pouvant être indispensables à l'exercice de ses activités ou simplement utiles en tant qu'éléments de preuve.
En cas de départ, les données professionnelles restent à la disposition de l'Université.

L'utilisateur est responsable de son espace de données à caractère privé et il lui appartient de le détruire au moment de son départ.

Adresses mail fonctionnelles

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place et être exploitée par un service ou un groupe d'utilisateurs. Chaque utilisateur ayant accès à cette boîte est alors responsable de son contenu.

Compromission d'un compte mail

Si l'utilisateur s'aperçoit que son mot de passe a été dérobé ou qu'un tiers a accès à ses messages, il modifie immédiatement son mot de passe et prévient le service informatique.
En effet, une adresse mail piratée est généralement utilisée pour envoyer un grand nombre de messages non sollicités (spam). Les prestataires de services de messagerie placent alors les serveurs de l'Université sur une liste noire, qui peut entraîner le blocage de tous les messages en provenance de l'Université.
Pour prévenir de tels dysfonctionnements, une limite technique est mise en œuvre par le service informatique : en cas d'abus, le compte de l'expéditeur est bloqué.

S'il est nécessaire de diffuser des messages à de très nombreux destinataires, il est impératif d'utiliser les listes de diffusion, qui ne provoquent aucune perturbation.

Surveillance du réseau

Les utilisateurs sont informés que l'Université 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 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 informatique.
Les administrateurs du réseau sont autorisés, en cas de difficultés majeures, à arrêter les services réseaux et à isoler les zones à risque.

4.2 Contenu des échanges par courriel

Netiquette

En toutes circonstances, l'utilisateur doit adopter un comportement responsable et respectueux des dispositions contenues dans la présente Charte.
Les échanges électroniques (courriers, forums de discussion, messagerie instantanée, réseaux sociaux, partages de documents, voix, images, vidéos, etc.) respectent la correction normalement attendue dans tout type d'échange tant écrit qu'oral.
L'utilisateur doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, pédophile, diffamatoire. Les auteurs de messages contenant de telles mentions sont susceptibles de faire l'objet de poursuites pénales ainsi que de poursuites disciplinaires par l'établissement.
Plus généralement, les messages électroniques dont le contenu comporte des mentions contraires aux bonnes mœurs, portant atteinte à la vie privée ou à l'image d'autrui, ou contrevenant au droit d'auteur sont interdits.

Caractère probant des courriels

Les informations échangées par voie électronique avec des tiers peuvent, au plan juridique, former un contrat sous certaines conditions ou encore être utilisés à des fins probatoires.

L'utilisateur doit, en conséquence, être prudent sur la nature des informations qu'il échange par voie électronique au même titre que pour les courriers traditionnels.
L'utilisateur est informé que le courriel est un document administratif pouvant être reconnu en tant que preuve en cas de contentieux.

Vigilance

L'utilisateur fait preuve de vigilance vis-à-vis des informations reçues (désinformation, virus, tentative d'escroquerie, chaînes, hameçonnage, …).
Il s'assure de l'identité et de l'exactitude des adresses des destinataires des messages.
Il est prudent vis-à-vis des liens présents dans les messages, renvoyant vers internet.
Il n'ouvre pas de fichiers en provenance d'un expéditeur inconnu, en particulier les fichiers compressés ou exécutables dont l'ouverture peut notamment générer l'activation de virus, de codes malveillants susceptibles d'entraîner des conséquences d'une extrême gravité pour l'Université
Les messages publicitaires et les spams reçus doivent être supprimés, si possible sans les ouvrir.
Les mails destinés à nuire (tels que le hameçonnage ou *phishing*) doivent être signalés au service informatique.

4.3 Bonnes pratiques - Droit à la déconnexion

Le courriel donne très souvent lieu à une consultation – voire une réponse – immédiate qui peut perturber l'organisation de notre travail.
Préciser l'usage du courriel doit permettre, d'une part, d'optimiser notre gestion du temps et donc d'améliorer notre efficacité collective et individuelle et d'autre part, de préserver notre disponibilité pour gérer d'autres tâches professionnelles (réunions, rendez-vous extérieurs, etc.).

Par ailleurs, chacun bénéficie d'un droit à la déconnexion permettant de protéger sa vie privée en dehors des heures de travail.

Un « Guide des bonnes pratiques de la messagerie » a été rédigé et est accessible sur le lien suivant

Droit à la déconnexion

L'Université fait appel à la responsabilité de chacun et à l'exemplarité des utilisateurs pour faire un usage approprié des outils numériques mis à leur disposition. L'usage de la messagerie et de tout autre outil n'a pas vocation à se substituer au dialogue et aux échanges de vive voix, qui renforcent le lien social et préviennent l'isolement.

En dehors des temps et lieux de travail, tout utilisateur reste libre de se connecter, ou non, aux outils de communication mis à disposition par l'Université. En revanche, il ne peut pas se voir reprocher de ne pas les avoir utilisés.

Pour le personnel d'encadrement, il est recommandé de restreindre l'envoi de mails en dehors des plages de travail. En tout état de cause les collègues ne sont pas tenus de consulter leurs mails en dehors des heures de travail, ni a fortiori d'y répondre.

Quelques bonnes pratiques

Un aperçu des recommandations figurant dans le « Guide des bonnes pratiques de la messagerie » est résumé ci-dessous :

- Vérifiez la pertinence du média utilisé : le téléphone ou un face-à-face sont parfois plus pertinents qu'un courriel ;

- Prêtez attention au moment le plus opportun pour l'envoi, évitez le sentiment d'urgence ;
- Limitez les destinataires aux personnes dont vous attendez une réponse ou une action ;
- N'attendez pas de réponse ou d'action des personnes en copie ;
- Evitez par exemple d'utiliser « Répondre à tous » ;
- Limitez la taille de l'email, donnez un lien plutôt que d'insérer une pièce jointe ;
- Rédigez avec soin, assurez-vous de toujours rester courtois ; attention aux majuscules, aux caractères en gras ou en couleur ;
- Assurez-vous que votre courriel comporte un objet clairement identifiable ;
- Ne laissez pas un échange par mail s'envenimer, parlez-en directement avec votre interlocuteur ;
- Dans votre boîte de réception, exploitez les fonctionnalités de filtres et de tri pour gagner du temps ;
- Lors d'une période de congés, activez la fonction de gestion des messages en cas d'absence (répondeur) ;
- Pour faciliter le fonctionnement des services, étudiez la possibilité d'utiliser une adresse courriel générique du type service_xyz@univ-paris1.fr plutôt qu'une adresse nominative.

Restez en toutes circonstances vigilants vis-à-vis du risque de mails malicieux (hameçonnage ou *phishing*), porteurs de virus, de liens vers des sites malveillants (vous demandant des informations confidentielles, un paiement immédiat, l'appel d'un numéro surtaxé, etc.).

5 Postes de travail

L'Université peut mettre à disposition de ses utilisateurs des postes de travail informatiques. Selon le profil de l'utilisateur, il peut s'agir de postes en libre-service (étudiants) ou de postes fixes ou portables affectés à l'utilisateur (personnel).
Ces postes de travail sont destinés à un usage professionnel.
De façon générale, ces postes sont fournis et maintenus par le service informatique de l'Université.

5.1 Postes en libre-service

Les postes en libre-service sont réservés à un usage professionnel.
Pour garantir la traçabilité des usages, il est obligatoire de s'authentifier à l'aide de son mot de passe, ou de noter sa session sur un registre prévu à cet effet.
L'utilisateur s'engage à faire un usage loyal et respectueux du poste de travail mis à sa disposition. Il n'en modifie pas la configuration ni la sécurité, et n'installe aucun logiciel sauf autorisation expresse.
Il ne laisse pas accès à des informations non publiques. En quittant son poste de travail, il veille à fermer sa session et à supprimer toute trace personnelle.

5.2 Autres postes de travail

Sécurité matérielle

L'utilisateur protège les équipements mis à sa disposition :

- il utilise les moyens de protection disponibles (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) pour garantir la protection des équipements mobiles et des informations qu'ils renferment (ordinateur portable, clé USB, smartphones, tablettes, etc.) contre le vol ;
- en cas d'absence, même momentanée, il verrouille ou ferme toutes les sessions en cours sur son poste de travail ;

- il signale le plus rapidement possible au service informatique toute perte, tout vol ou toute compromission suspectée ou avérée d'un équipement mis à sa disposition.

Sécurité logicielle

L'utilisateur applique les consignes de sécurité informatique de l'établissement afin de s'assurer notamment que la configuration de son équipement suit les bonnes pratiques de sécurité (application des correctifs de sécurité, pare-feu, chiffrement, etc.) ;

- il doit suivre les règles en vigueur au sein de l'Université pour toute installation de logiciel. Il ne doit pas installer de logiciels autres que ceux prévus par sa composante ou son service ni contourner les restrictions d'utilisation d'un logiciel ;
- l'Université a déployé une protection logicielle généralisée de type anti-virus sur les postes de travail des utilisateurs. Il est interdit de désactiver, d'altérer le fonctionnement ou de désinstaller ce logiciel anti-virus ;
- l'Université a déployé des systèmes de mise à jour de sécurité du poste. Il est interdit de désactiver ces systèmes ou d'altérer le fonctionnement de ces mises à jour.

Périphériques de stockage

Les périphériques de stockage comme les clés USB, les disques durs externes - voire les téléphones portables que l'on connecte à son poste de travail - sont un vecteur fréquent d'introduction de logiciels malveillants sur le réseau de l'Université.
Un périphérique de stockage d'origine inconnue peut non seulement contenir des virus, mais également être configuré pour « aspirer » le contenu du poste de travail à l'insu de son propriétaire.

- il est recommandé de privilégier les périphériques fournis par l'Université ;
- l'usage de périphériques d'origine privée, apporté par l'utilisateur est toléré mais doit faire l'objet de la plus grande vigilance ;
- il est recommandé de séparer les usages entre les périphériques de stockage professionnels et privés ;
- il est strictement interdit de connecter à un poste de travail un périphérique trouvé par terre, près d'un poste, ou sans origine connue. En effet, la mise à disposition de clés « abandonnés » infectées est un moyen couramment utilisé pour propager un logiciel malveillant. Les clés USB trouvées doivent être remises au service informatique, qui pourra s'assurer de leur innocuité et rechercher leur propriétaire éventuel.

Équipements nomades

Lorsqu'un équipement nomade, de type ordinateur portable, tablette, téléphone mobile, projecteur, périphérique de visio-conférence, etc. est confié à un utilisateur :

- cette mise à disposition est réputée intervenir dans le cadre exclusif des activités professionnelles du bénéficiaire ;
- elle entraîne l'obligation pour le bénéficiaire d'apporter tous les soins nécessaires à la bonne conservation de ce matériel tels que ne pas exposer l'équipement confié à la chaleur ni à l'humidité ;
- l'utilisateur reste responsable du matériel prêté, ne doit à aucun moment le laisser sans surveillance, et doit ranger le matériel non-utilisé dans un endroit sécurisé.

Administration des postes

Les administrateurs du service informatique peuvent, en cas de dysfonctionnement technique, d'intrusion ou de tentative d'attaque sur les systèmes informatiques utiliser les journaux ou traces présentes sur un poste de travail pour tenter de retrouver l'origine du problème. Ces personnels sont soumis à une obligation de confidentialité.

Ils ne peuvent pas prendre connaissance du contenu des répertoires, fichiers ou messages explicitement désignés comme privés ou personnels, sauf en cas d'urgence justifiée, en présence de l'agent et avec son autorisation expresse.
Pour effectuer des actions de maintenance corrective, curative ou évolutive, l'Université peut déclencher des mises à jour à distance sur les postes connectés à son réseau. Si une maintenance nécessite une prise de contrôle du poste à distance, elle se fait après accord de l'utilisateur et en sa présence.
Si l'utilisateur d'un poste informatique de l'Université est suspecté d'avoir une utilisation non appropriée de son poste (par exemple consultation fréquente et prolongée de sites pornographiques), le directeur du service ou de la composante concernée peut demander par écrit à la DSIUN un audit du poste concerné. L'inspection des journaux du poste informatique, ou l'inspection des connexions du poste vers internet recueillies à l'occasion de cet audit se fera alors en présence de l'agent et du directeur du service.

Navigation sur 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.
Il convient de faire preuve de prudence, s'abstenir de se connecter à des sites suspects et éviter de télécharger des logiciels dont l'innocuité n'est pas garantie ; par exemple : vérifier la pérennité du logiciel et / ou la nature de l'éditeur.
Les utilisateurs sont invités à privilégier la navigation en mode « privé », option disponible sur tous les navigateurs proposés par le service informatique. Ce mode limite le stockage des données de navigation et des « cookies ».

Sauvegarde de données

L'Université met à disposition de ses utilisateurs des répertoires personnels ou partagés, dont elle assure la sauvegarde par l'intermédiaire de son réseau.
Leur utilisation doit être privilégiée.
Si l'utilisateur stocke des données sur d'autres espaces de stockage qui lui sont propres, il lui appartient d'en assurer la sauvegarde régulière.
Une sauvegarde régulière est l'unique moyen de garantir la pérennité des données et de se prémunir contre les conséquences néfastes d'un problème technique, d'un vol ou d'une attaque informatique de type « rançongiciel » (ou *ransomware)*.

Continuité de service : gestion des absences et des départs

Les données professionnelles restent à la disposition de l'employeur. Les mesures de conservation des données professionnelles sont définies avec le responsable hiérarchique. L'utilisateur doit mettre en œuvre les mesures nécessaires pour permettre l'accès à ses données professionnelles en vue de garantir la continuité de service en cas d'absence. Ces mesures peuvent être l'utilisation de répertoires partagés, de systèmes de gestion électronique de documents, d'utilisation d'adresses mail génériques partagées avec d'autres collègues, ou tout simplement un message d'absence sur sa messagerie.

En cas de départ définitif ou de changement de poste, l'utilisateur :

- demande au service informatique la suppression des droits d'accès aux applications et aux répertoires qui étaient liés à sa mission
- demande la désinscription de son adresse électronique des différentes listes de diffusion liées à sa mission
- s'assure que ses données professionnelles ont été triées et classées, et sont accessibles par sa hiérarchie ou ses collègues

- se charge de la suppression de ses données personnelles

5.3 Utilisation privée d'un poste de travail

Les ressources informatiques (postes de travail, serveurs, applications, messagerie, accès internet, téléphone, etc.) fournies à l'utilisateur sont réservées à l'exercice de son activité professionnelle.

Tolérance d'un usage privé

Un usage personnel du poste de travail est toutefois toléré à condition :

- qu'il reste limité, tant dans la fréquence que dans la durée ;
- qu'il ne mette pas en danger son bon fonctionnement et sa sécurité ;
- qu'il n'affecte pas l'usage professionnel ;
- qu'il reste non lucratif
- qu'il n'enfreigne pas la loi, les règlements et les dispositions internes.

Données à caractère privé

Toute donnée est réputée professionnelle à l'exception des données explicitement désignées par l'utilisateur comme ayant un caractère privé par la mention « Privé » ou « Personnel ».
L'utilisateur procède au stockage de ses données à caractère privé dans un espace de données prévu à cet effet ou en mentionnant explicitement le caractère privé sur la ressource utilisée. Ceci peut être fait en nommant le répertoire concerné « Privé » ou « Personnel », complété de son nom.
Cet espace ne doit pas contenir de données à caractère professionnel et il ne doit pas occuper une part excessive des ressources. La protection et la sauvegarde régulière des données à caractère privé incombent à l'utilisateur.
Le personnel du service informatique n'est pas autorisé à prendre connaissance du contenu des répertoires, fichiers ou messages explicitement désignés comme personnels, sauf en cas d'urgence justifiée (par exemple suite à un problème de sécurité grave), en présence de l'agent et avec son autorisation expresse.

Suppression des données à caractère privé

La sauvegarde régulière des données à caractère privé incombe à l'utilisateur.
A son départ de l'Université, l'utilisateur est responsable de la suppression des données privées qu'il aurait stockées dans le système d'information de l'établissement.

5.4 Utilisation du poste en mode administrateur

Pour des besoins particuliers, certains utilisateurs peuvent disposer d'un compte avec des droits d'administrateur local sur leur poste.
Dans ce cas, l'utilisateur est responsable de la gestion des mises à jour et la surveillance des alertes émises par les dispositifs de protection antivirale, ainsi que du bon fonctionnement général de son poste. Une charte spécifique « Charte de délégation des droits d'administration des postes », qu'il signe, formalise alors ses droits et ses responsabilités, et attire son attention sur les risques encourus.

L'utilisation de ce compte doit être réservée aux actions d'administration qui le nécessitent. Pour les autres usages, et particulièrement pour la navigation sur internet, il est obligatoire d'être connecté via son compte standard, ne possédant pas les privilèges « administrateur ». En effet, les comptes administrateurs sont les cibles privilégiées de nombreux programmes malveillants tentant d'accéder aux ressources du poste, avec des droits élevés.

5.5 Connexion d'un matériel personnel au réseau

La connexion d'un matériel personnel au réseau Wi-Fi est autorisée, dans la mesure où elle a une finalité professionnelle. Un usage personnel est toléré dans la mesure où il reste modéré.
Les services offerts aux matériels ainsi connectés sont limités, ne permettant pas l'accès à certaines ressources telles que par exemple des répertoires partagés.

La connexion filaire (c'est-à-dire sur une prise réseau) d'un matériel personnel doit faire l'objet d'une demande préalable au service informatique. A partir du moment où ces matériels accèdent à des données professionnelles ou les stockent, ils doivent faire l'objet d'attentions particulières et de mesures de sécurité renforcées. Ils ne doivent pas remettre en cause ou affaiblir la sécurité du réseau de l'Université.
En tout état de cause, pour le personnel, les usages professionnels et personnels doivent être clairement séparés.

De nombreux services, tels que les applications métiers de l'Université, ne sont accessibles qu'à partir d'un poste fourni et administré par l'Université.

5.6 Télétravail

L'Université peut autoriser son personnel à pratiquer le télétravail depuis son domicile.
L'accès au réseau de l'Université et aux applications se fait alors selon une procédure spécifique, garantissant la sécurité des échanges. Certaines applications ou certains services peuvent ne pas être accessibles en télétravail.
La présente Charte reste applicable dans le cadre du télétravail. Les consignes spécifiques de sécurité sont données à l'occasion de la formation des agents au télétravail et rappelées dans les documents qui leur sont remis.

5.7 Téléphone

L'Université peut mettre à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.
L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.

Des restrictions d'utilisation par les utilisateurs des téléphones fixes sont mises en place en tenant compte de leurs missions. A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

Des logiciels présents sur les postes de travail peuvent offrir les mêmes fonctionnalités. De même, des équipements spécifiques de visio-conférence peuvent être mis à disposition.

L'Université n'a pas mis en œuvre de suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs. L'Université s'interdit d'accéder à l'intégralité des numéros appelés via l'autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, l'Université, sur demande du ou de la DGS, se réserve le droit d'accéder aux numéros complets des relevés individuels.

6 Informatique et libertés

6.1 Droits d'accès

L'Université s'est dotée d'un Délégué à la Protection des Données (anciennement Correspondant Informatique et Libertés ou CIL), chargé de s'assurer de la bonne application de la réglementation « Informatique et Libertés » en son sein.

Conformément aux dispositions de cette loi et du règlement européen sur la protection des données, chaque utilisateur dispose d'un droit d'accès, de rectification, d'opposition, de limitation et de portabilité relatif à l'ensemble des données personnelles le concernant. Ce droit s'exerce auprès du Délégué à la Protection des Données de l'établissement : dpo@univ-paris1.fr .

6.2 Créations de fichiers nominatifs

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, 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 «Informatique et Libertés» et le Règlement Général sur la Protection des Données européen.
Tout utilisateur souhaitant procéder à un tel traitement devra prendre contact préalablement le Délégué à la Protection des Données (DPO) qui définira avec lui les mesures nécessaires au respect des dispositions légales.

6.3 Mesures de garantie du bon fonctionnement et contrôle de la sécurité

Journalisation des accès

L'Université est dans l'obligation légale de mettre en place un système de journalisation des accès à son réseau, dans la mesure où il permet l'accès à internet. Ces données restent confidentielles, et ne sont accessibles qu'aux administrateurs du réseau désignés par l'Université.
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.
Les sites internet accédés ou les mails échangés ne font pas l'objet d'une journalisation.

Garantie de bon fonctionnement et de la sécurité

L'Université se réserve le droit de réduire ou supprimer l'accès au réseau d'une machine présentant un comportement anormal, tel que la diffusion de virus sur le réseau.
Elle peut bloquer l'accès à des adresses mails ou à des sites étant répertoriés comme malveillants.
Tout échange de fichiers ou de courriels présentant une difficulté technique bloquante d'acheminement à son destinataire peut être isolé, le cas échéant supprimé.

L'Université informe l'utilisateur que le système d'information fait l'objet d'une surveillance de bon fonctionnement, incluant des mesures à des fins statistiques, de traçabilité, d'optimisation, de

sécurité ou de détection des abus. Ces mesures sont chaque fois que possible anonymisées. Les personnels chargés des opérations de contrôle sont soumis au secret professionnel.

Demande de réquisition judiciaire

Dans le cas d'une réquisition judiciaire, l'Université sera tenue de communiquer, ou d'exploiter pour recherche, toutes les traces contenue dans ses journaux concernant la ou les personnes incriminées.

7 Rappel de la législation applicable

L'utilisateur est tenu de respecter la législation française notamment les textes ci-dessous.

Législation relative à la propriété intellectuelle

L'utilisateur respecte les dispositions du code de la propriété intellectuelle (notamment les articles L111-1 et L112-2) relatives à la propriété littéraire et artistique. L'utilisateur ne fait pas de copies illicites d'éléments (logiciels, images, textes, musiques, sons, etc.) protégés par les lois sur la propriété intellectuelle
L'utilisateur ne reproduit pas, ne télécharge pas, ne copie pas, ne diffuse pas, ne modifie ni n'utilise les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation écrite des titulaires de ces droits.
Il utilise les logiciels dans le strict respect des licences souscrites, toute copie autre qu'une copie de sauvegarde étant considérée comme une contrefaçon (article L335-3).
Par ailleurs des systèmes anti plagiat sont mis en œuvre au sein de l'Université.

Limites à la liberté d'expression

La loi du 29 juillet 1881 sur la liberté de la presse et divers textes publiés depuis cette date règlementent la liberté d'expression.
L'utilisateur ne diffuse pas des informations constituant des atteintes à la personnalité (injure, discrimination, racisme, xénophobie, révisionnisme, diffamation, obscénité, harcèlement ou menace) ou pouvant constituer une incitation à la haine ou la violence, ou une atteinte à l'image d'une autre personne.

Loi Informatique et Libertés du 6/1/1978 et règlement européen 2016/679

L'utilisateur respecte la réglementation relative au traitement des données à caractère personnel (notamment la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) ; le Règlement Général sur Protection des Données (RGPD), à l'échelle européenne, vient renforcer cette législation et s'applique à partir du 25/05/2018.
Le droit à la protection de la vie privée et le droit à l'image sont également applicables (article 9 du code civil).

Secret des correspondances privées

La violation du secret de la correspondance est sanctionnée (article 226-15 et 432-9 du code pénal).
La notion de correspondance privée est définie par une circulaire du 17 février 1988.

Pédopornographie

La consultation ou la détention d'images pédopornographiques est sévèrement réprimée par les articles L227-23 du code pénal. L'Université a de plus un devoir de dénonciation aux pouvoirs publics (article 40 du code de procédure pénale) de tout utilisateur détenant de telles images.

Atteinte aux systèmes automatisés de données

L'utilisateur respecte la législation relative aux atteintes aux systèmes de traitement automatisé de données (art. L 323-1 à 323-7 du code pénal).
Il n'accède ni ne se maintient dans un réseau frauduleusement, n'entrave pas le fonctionnement d'un système, ni ne modifie frauduleusement des données.

Autres :

On peut également citer, sans que ce soit exhaustif :

- La loi n° 94-665 du 4 août 1994 modifiée relative à l'emploi de la langue française ;
- La législation applicable en matière de cryptologie : articles 30 à 36 de la loi 2004-575 du 21 juin 2014 pour la confiance dans l'économie numérique ;
- Les dispositions relatives à la Protection du Potentiel Scientifique et Technique de la Nation. Certaines de ces dispositions sont assorties de sanctions pénales ;
- Les obligations de secret professionnel et de discrétion professionnelle (loi 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires) ;
- L'article L. 34-1 du Code des Postes et Communications Electroniques sur la protection de la vie privée des utilisateurs de réseaux et services de communications électroniques ;
- Le respect de la vie privée et notamment l'interdiction de filmer ou d'enregistrer une personne sans son accord préalable ;
- Les mesures de respect de l'ordre public.

8 Divers

8.1 Applicabilité

La présente Charte s'applique à l'ensemble des personnels et utilisateurs de l'Université, c'est-à-dire à l'ensemble des personnes utilisant les moyens informatiques de l'Université ainsi que ceux auxquels il est possible d'accéder à distance à partir du réseau de l'Université.
Elle s'applique en outre à toutes les personnes accueillies à l'Université et ayant accès à son réseau ou à ses services numériques.
La présente Charte faisant partie du règlement intérieur, elle s'applique sans qu'il y ait besoin d'une acceptation formelle de l'utilisateur. Dans un objectif d'information et de sensibilisation, il est demandé à chaque utilisateur d'accepter numériquement la Charte lors de l'activation de son compte.

8.2 Entrée en vigueur de la Charte

La présente Charte est annexée au règlement intérieur de l'Université.
Elle se substitue à la précédente « Charte pour l'utilisation des ressources informatiques et des services internet ».
Elle entre en vigueur le 13/12/2018, jour de son adoption par le Conseil d'Administration de l'Université.

8.3 Limitations et sanctions applicables

En cas de non-respect par un utilisateur des règles définies dans la présente Charte, le Directeur des Systèmes d'Information et des Usages Numériques pourra déconnecter l'utilisateur, avec ou sans préavis selon la gravité de la situation, ou limiter ses accès pour une durée déterminée.

Le Directeur Général des Services ou le Président pourra, après en avoir averti l'intéressé et sans préjuger des poursuites ou procédures de sanction pouvant être engagées à son encontre, limiter les usages par mesure conservatoire, interdire à l'utilisateur l'accès à des ressources (par exemple l'accès à internet), ou retirer les droits ou autres dispositifs de contrôle d'accès et fermer les comptes.

8.4 Autres chartes

Des chartes plus spécifiques, ou des documents complémentaires ont été rédigés pour répondre à un certain nombre de cas particuliers :

- Guide des bonnes pratiques de messagerie
- Charte d'utilisation des EPI
- Engagement de confidentialité / Charte des prestataires

- Charte de bon usage pour les élus
- Charte de bon usage pour les élus étudiants
- Charte de bon usage pour les associations étudiantes
- Charte de bon usage pour les listes de candidats aux élections aux conseils centraux
- Charte de bon usage pour les syndicats

- Charte de délégation des droits d'administration des postes
- Charte d'accès distant à un poste de travail
- Charte de l'accès à internet pour les personnels logés de l'Université
- Charte du Web et des réseaux sociaux
- *Charte des administrateurs informatiques (à venir)*

8.5 Aide-mémoire des droits et obligations

L'aide-mémoire des droits et obligations ci-dessous reprend sous une forme synthétique les principaux points de la présente Charte. D'autres guides ou aide-mémoire, destinés à la sensibilisation, pourront être rédigés ultérieurement.

La Charte concerne tout usager des ressources numériques de l'Université : étudiants, enseignants, personnel administratif, lecteurs, …

En tant qu'usager de l'Université, j'ai le droit :

- d'accéder au réseau de l'Université, en Wifi ou via une prise dans mon bureau selon mon statut
- de détenir un compte usager, qui me permet d'accéder à des applications
- d'avoir un compte mail se terminant par univ-paris1.fr ou pantheonsorbonne.fr
- d'accéder à un poste de travail en libre-service (étudiants) ou d'avoir l'usage d'un poste à mon bureau (personnel administratif)

En tant qu'usager de l'Université, j'ai le devoir :

- de réserver ces services à un usage professionnel ou au cadre des études ; un usage personnel résiduel est toléré, et ne doit apporter aucune perturbation à leur fonctionnement.
- de garder secret le mot de passe qui m'est fourni
- de le changer si je pense qu'il a été divulgué
- de respecter les droits d'accès associés à mon compte sans chercher à les contourner
- de rester courtois et respectueux dans mes mails professionnels
- de faire preuve de vigilance vis-à-vis des mails malveillants
- de respecter les règles liées au matériel que j'utilise :
  - ✓ de m'identifier pour utiliser les services offerts
  - ✓ de respecter la configuration du poste sans chercher à la modifier
  - ✓ de ne pas chercher à installer moi-même un logiciel
  - ✓ de façon générale, de prendre soin du matériel qui m'est confié

  et pour les postes de travail du personnel administratif
  - ✓ d'identifier clairement mes fichiers ou mes mails personnels éventuels
  - ✓ si on me confie un poste portable ou nomade, de le protéger contre le vol
- de m'abstenir de toute action malveillante vis-à-vis du réseau, des services ou des matériels de l'université ; pour assurer leur sécurité, mes accès peuvent être tracés
- de protéger les données personnelles des tiers