



CHARTRE RELATIVE À L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION A L'UNIVERSITE DU HAVRE

La présente charte a pour objet de définir les règles d'utilisation des technologies de l'information et de la communication - et des ressources informatiques afférentes - au sein de l'Université du Havre.

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

1. Champ d'application de la charte

1.1 / Définition des utilisateurs

Sont désignées dans la présente charte comme « utilisateurs », l'ensemble des personnes autorisées à accéder aux ressources informatiques de l'établissement.

1.2 / Périmètre des ressources informatiques

Les ressources informatiques comprennent de façons non exhaustives les services, les serveurs, les postes de travail, les appareils communicants des services administratifs, des bureaux, des salles pédagogiques, des laboratoires et des centres de documentation de l'Université.

1.3 / Droit d'accès aux ressources informatiques

L'accès aux ressources informatiques de l'Université comprend :

- l'accès au matériel informatique de l'Université ;
- l'accès aux logiciels à usage professionnel ou pédagogique ;
- l'accès au réseau filaire et Wi-Fi mis à disposition par l'Université ;
- l'accès distant aux ressources de l'Université via Internet, par exemple via le portail ENT (Environnement Numérique de Travail).

L'Université met à la disposition des utilisateurs des moyens d'accès aux ressources informatiques. Ceux-ci, de quelque nature qu'ils soient (mot de passe, carte à puce ...), sont strictement personnels et inaccessibles.

2. Conditions d'accès aux ressources informatiques de l'Université

Le réseau informatique de l'Université du Havre est relié au réseau régional SYRHANO (Système Réseau de Haute-Normandie) grâce auquel il est possible d'accéder à RENATER (Réseau National pour la Technologie, l'Enseignement et la Recherche) et à l'Internet.

Les zones Wi-Fi dans l'établissement sont une extension du réseau filaire classique mais, bien qu'elles en aient les mêmes capacités, elles n'en possèdent pas les performances. Les débits de connexion sont moindres que sur un réseau câblé. De par sa conception de réseau partagé, les débits du Wi-Fi sont inversement proportionnels au nombre de personnes connectées sur une zone. Afin de ne pas pénaliser les autres utilisateurs utilisant la même borne Wi-Fi, le téléchargement de fichiers volumineux est à proscrire.

3. Sécurité et bon fonctionnement des ressources informatiques

3.1 / Dispositions nécessaires pour la sécurité et le bon fonctionnement du système d'information

L'Université s'efforce, dans la mesure de ses possibilités, de prendre les dispositions nécessaires pour assurer la sécurité et le bon fonctionnement de ses ressources informatiques. Elle peut en particulier :

- Surveiller les débits ;
- Changer la priorité ou stopper l'exécution d'une tâche lancée par un utilisateur ;

- Retirer le droit d'accès d'un utilisateur ;
- Procéder au contrôle à priori ou a posteriori des sites visités et des durées d'accès correspondantes ;
- Filtrer ou interdire l'accès à certains sites présentant un risque pour la sécurité des systèmes d'information.

La décision d'effacer un fichier ne peut être prise qu'après information à l'utilisateur concerné.

L'Université peut toutefois prendre toutes les mesures nécessaires afin d'assurer la pérennité et la continuité du service en prenant toute mesure visant à préserver le bon fonctionnement et la disponibilité normale des moyens informatiques qui leurs sont confiés. A ces conditions, il peut être dérogé à l'obligation d'information en cas d'effacement de fichiers ou données.

3.2 / Téléchargement

Tout téléchargement de fichiers sur internet, notamment de sons ou d'images, doit s'effectuer dans le respect des droits de la propriété intellectuelle.

L'Université se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'informations (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'Université, codes malveillants, programmes espions...).

3.3 / Fichiers de traces

L'Université dispose, pour des raisons techniques, de « fichiers de traces » qui concernent des informations relatives à certains usages des ressources du système d'information, tels que les accès Internet, la messagerie et les données échangées.

A cet effet, l'Université se réserve le droit de mettre en place des outils de traçabilité sur toutes les ressources du système d'information.

Ces fichiers ne sont utilisés que pour un usage technique, afin de remédier à certains dysfonctionnements.

Toutefois, dans le cadre d'une procédure judiciaire, ces fichiers peuvent être mis à la disposition de la justice.

4. Droits et responsabilités des utilisateurs

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques. Il s'engage à n'effectuer aucune opération qui pourrait nuire au fonctionnement normal du réseau, à l'intégrité des moyens informatiques, ou aux relations internes et externes de l'établissement.

L'Université du Havre ne peut être tenue pour responsable en cas de dommage ou perte de données d'un utilisateur découlant directement ou indirectement de l'utilisation de ses ressources informatiques.

Chaque utilisateur est responsable de la sécurité de ses propres fichiers. Il est recommandé à l'utilisateur de faire par ses propres moyens, la sauvegarde régulière des données jugées importantes (ou sensibles).

L'utilisateur doit respecter les modalités de raccordement des matériels au réseau informatique. Ces raccordements ne pourront pas être modifiés sans autorisation préalable.

Autres engagements de l'utilisateur :

a. Utilisation du code d'accès attribué à l'utilisateur

Chaque personne autorisée dite « utilisateur » se voit attribuer un compte informatique avec un code d'accès. Les codes d'accès ou mots de passe sont strictement personnels et confidentiels. Chaque utilisateur est responsable de l'utilisation qu'il en fait. Il s'engage en particulier à ne jamais communiquer son code d'accès et doit informer le Centre de Ressources Informatiques de toute anomalie qu'il pourrait constater.

b. Messagerie

L'Université s'engage à mettre à la disposition de l'utilisateur une boîte aux lettres nominative lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est de la responsabilité de l'utilisateur.

La messagerie est un outil de travail ouvert à des usages professionnels et pédagogiques : elle peut constituer le support d'une communication privée (usage restreint).

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

c. *Respect de la propriété intellectuelle*

L'utilisation des logiciels (notamment des bases de données, photographies, images, pages web, extrait musical, extraits littéraires ...) à l'Université du Havre doit se faire dans le respect de la propriété intellectuelle (loi 92-597 du 1er juillet 1992)

La reproduction, la modification, la copie, la diffusion ou l'utilisation de logiciels ou autres ressources numériques protégées par un droit d'auteur ou un droit privatif nécessite une autorisation préalable des titulaires de ces droits.

L'utilisateur s'engage notamment à ne pas effectuer intentionnellement les actions suivantes :

- de détériorer les locaux où sont entreposé du matériel informatique ;
- d'usurper l'identité d'un tiers ;
- d'intercepter toutes communication entre tiers ;
- d'accéder aux données d'un autre utilisateur sans son autorisation ;
- de faire une utilisation abusive des ressources informatiques partagées ;
- la vente de service sans rapport avec l'enseignement ou la recherche ;
- d'interrompre ou d'altérer le fonctionnement normal du réseau informatique.

d. *Devoir de signalement et d'information*

Les utilisateurs qui constatent une dégradation ou un dysfonctionnement des outils informatiques doivent, dans les plus brefs délais, informer le Centre de Ressources Informatiques.

Il doit également informer toute anomalie découverte telle une intrusion dans le système d'information, de toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation et de toute utilisation frauduleuse de son identité numérique.

5. Utilisation d'un ordinateur ou autre matériel communicant (hors ceux mis à la disposition des usagers par l'Université) sur le réseau informatique de l'établissement

L'utilisateur souhaitant utiliser son ordinateur ou autre matériel communicant "personnel" sur le réseau informatique de l'établissement doit exclusivement utiliser les réseaux Wi-Fi de l'Université ou si possible, un réseau filaire dédié soumis à authentification de l'utilisateur, après accord préalable du Centre de Ressources Informatiques.

L'utilisateur doit faire tout le nécessaire afin de garantir la sécurité de son matériel (utilisation d'un antivirus avec signatures récentes, mises à jour régulières de ses différents logiciels et système d'exploitation...).

6. Droits d'administrateur pour l'utilisation de son ordinateur professionnel

Obtenir les droits d'administrateur pour l'utilisation de son ordinateur professionnel de l'Université du Havre doit être l'exception et non la règle.

Toute demande en ce sens doit donc être motivée. Si la demande est acceptée, l'utilisateur renonce à la maintenance de son matériel par le Centre de Ressources Informatiques.

En outre, il doit notamment s'engager à mettre tout en œuvre pour garantir la sécurité de son matériel (utilisation d'un antivirus avec signatures récentes, mises à jour régulières de ses différents logiciels et système d'exploitation...).

7. Données à caractères personnels (ou privés)

L'utilisation des systèmes d'information à titre privé doit respecter la réglementation en vigueur.

Bien que les systèmes d'information soient réservés à un usage professionnel, leur utilisation à des fins « non professionnelles », pour répondre ponctuellement à des obligations socialement admises, est tolérée. L'usage des systèmes d'information se traduit dans les faits par :

- la possibilité de créer un répertoire informatique non professionnel.
- la possibilité d'utiliser l'adresse électronique à des fins non professionnelles.

Pour ce faire, les répertoires, fichiers ou correspondances émises ou reçues devront être clairement identifiés comme « non professionnels ». Dans cette circonstance, il est de la responsabilité de l'utilisateur de créer un répertoire informatique intitulé « **privé** » ou « **personnel** ». De même, les courriers électroniques émis ou reçus devront comporter dans l'objet du message la mention « **privé** » ou « **personnel** » et être conservé le cas échéant dans un répertoire intitulé « **privé** » ou « **personnel** » du système de gestion des courriels.

La responsabilité d'identification et la sauvegarde des données personnelles (privées) incombent au seul utilisateur.

Lors de son départ définitif de l'établissement, il appartient à l'utilisateur de détruire ses données à caractère privé, la responsabilité de l'établissement ne pouvant être engagée quant à la conservation de cet espace.

L'espace de données à caractère privé sera cependant détruit automatiquement, si l'utilisateur ne l'a pas fait lors de son départ.

8. Responsabilité de l'établissement et continuité de service

L'Université ne pourra être tenue pour responsable de détérioration d'informations du fait d'un utilisateur ne s'étant pas conformé aux règles énoncées dans la présente charte.

A la seule fin d'assurer la continuité de service, l'Université se réserve le droit d'accéder à l'ensemble des données professionnelles de l'utilisateur (dossiers, fichiers, courriels et plus généralement tous documents à caractère professionnel) après son départ définitif ou absence supérieure à 15 jours. De ce fait, l'Université peut en prendre connaissance ou consulter ces différents éléments, même en l'absence de l'utilisateur, en ayant notamment recours aux codes administrateurs systèmes.

Avant son départ temporaire ou définitif, l'utilisateur (personnel de l'établissement) doit informer sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition, afin d'assurer la continuité de service.

9. Télétravail

L'agent exerçant son activité selon les modalités propres au télétravail s'engage à respecter la présente charte, aussi bien dans les locaux de l'université que sur son lieu de télétravail.

Par ailleurs, pour des raisons de sécurité et à des fins de protection des données qu'il est susceptible de traiter dans le cadre de ses fonctions, il est rappelé ce qui suit :

- L'ordinateur professionnel utilisé dans le cadre du télétravail n'est en aucun cas un ordinateur familial. Aucun membre de la famille, ami ou tiers ne doit être autorisé à y accéder ;
- Le mot de passe permettant de déverrouiller l'ordinateur est strictement personnel à l'agent et ne doit pas être confié à autrui ;
- Le télétravailleur s'abstient de consulter des documents professionnels en présence d'autrui ;
- Afin d'assurer la sécurité des communications et des données, le télétravailleur ne doit pas installer de logiciels non autorisés.

10. Respect des lois et réglementations

Chaque utilisateur doit respecter la réglementation en vigueur.

Les principaux textes de référence (liste non exhaustive) :

- la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- la loi n°88-19 du 5 janvier 1988 relative à la fraude informatique ;
- la loi du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunication ;
- la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
- la loi 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information ;
- la circulaire n°2004-035 DU 18-2-2004 relative à l'usage de l'Internet dans le cadre pédagogique et protection des mineurs.

- les articles L.323-1 à 323-7 du code pénal relatifs à la répression des crimes et délits contre les biens ;
- les articles R624-3 et suivants du Code Pénal relatif à la sanction pénale de la diffamation ;
- les articles R226-1 et suivants, R623-4 et R625-9 du code pénal relatifs aux atteintes à la vie privée ;
- l'article 227-23 du Code Pénal, relatif à la sanction pénale de la consultation habituelle (sur Internet), de l'enregistrement, de la diffusion et de la détention d'images pédopornographiques ;
- les articles R625-7 et suivants relatifs du Code Pénal relatifs à la sanction pénale de l'incitation à la discrimination, à la haine ou à la violence ;

- l'article 9 du code civil relatif au droit à la vie privée ;
- les articles 1369-1 à 1369-11 du Code Civil relatifs aux contrats sous forme électronique ;

- les articles L335-2 et L335-3 du code de la propriété intellectuelle.

- Sont entre autres interdits :

a. Crimes et délits contre les personnes physiques et morales :

- porter atteinte à la vie privée d'un tiers ;
- porter atteinte à la sensibilité d'un tiers (par l'intermédiaire d'images, textes provocants, diffamatoires, discriminatoires, haineux ou injurieux) ;
- la dénonciation calomnieuse ;
- l'atteinte au secret professionnel ;
- porter atteinte aux droits de la personne ;
- la détention, diffusion et exportation d'images à caractère pédophile...

b. Crimes et délits contre les biens :

- l'escroquerie ;
- l'introduction frauduleuse d'un système de données (notamment de virus...) susceptibles d'entraver ou de fausser le fonctionnement normal d'une ressource informatique...

c. Infractions de presse (loi 29 juillet 1881. Modifiée) :

- la provocation aux crimes et délits ;
- l'apologie des crimes contre l'humanité ;
- l'incitation au terrorisme ;
- la diffusion de contenus à caractère raciste ou antisémite ;
- la diffamation ;
- l'injure ...

d. Infraction au code de la propriété intellectuelle :

- la violation des droits d'auteur (contrefaçon d'une œuvre de l'esprit...) ;
- la contrefaçon de marque...

Si un utilisateur doit, dans l'accomplissement de ses missions, constituer des fichiers de données nominatives faisant l'objet d'un traitement automatisé, il doit au préalable saisir le Correspondant Informatique et Libertés (CIL) désigné par l'établissement.

11. Respect de la charte informatique

L'utilisateur est tenu de respecter la présente charte, ainsi que la charte déontologique RENATER disponible sur le site <https://www.renater.fr/chartes>.

12. Sanctions

En cas de non-respect des règles définies dans le présent document, l'Université pourra suspendre immédiatement les droits d'accès de l'utilisateur aux ressources informatiques, de façon provisoire jusqu'au

prononcé de la décision définitive du président. Cette décision interviendra une fois que l'utilisateur aura été entendu.

Dans l'hypothèse où la violation en cause constituerait une faute passible d'une sanction disciplinaire, l'intéressé pourra se voir traduit devant l'instance disciplinaire compétente.

Le Havre, le

Affectation (composante, service, laboratoire) :

Nom et Prénom :

Signature (précédée de la mention « Lu et approuvé ») :