UNIVERSITÉ
CAEN
NORMANDIE

Charte relative à l'usage du système d'information et des technologies de l'information et de la communication à l'Université de Caen Normandie

Chapitre 1er - Objet de la charte, champ d'application

Article 1er - Objet

La présente charte définit les droits et obligations des utilisateurs du Système d'Information (SI) et des Technologies de l'Information et de la Communication (TIC) mis à disposition par l'Université de Caen Normandie (UNICAEN). Elle permet de garantir la sécurité et la maîtrise des ressources de l'établissement, de préserver son image d'assurer la protection de ses systèmes d'information et de respecter les droits de l'ensemble des utilisateurs. Elle respecte les dispositions législatives et réglementaires qui s'imposent à l'UNICAEN et aux utilisateurs.

Article 2 – Définition du SI et des TIC

On entend par système d'information et technologies de l'information et de la communication l'ensemble des moyens matériels, des logiciels, des bases de données, des réseaux de communication et des données pouvant être mis à disposition des utilisateurs.

L'accès à cet ensemble à distance, par un poste fixe ou par l'informatique « nomade » (ordinateurs portables, tablettes, téléphones mobiles, …) que ces matériels soient mis à disposition par l'université ou qu'il s'agisse de matériel personnel utilisé à des fins professionnelles, relève également de la présente charte, ainsi que toute nouvelle technologie de l'information ou de communication déployée par l'UNICAEN.

Article 3 – Définition des utilisateurs

On entend par utilisateur toute personne physique ou morale qui a accès à tout ou partie des moyens informatiques et de communications électroniques de l'université.

Il s'agit des personnels de l'établissement, des usagers du service public de l'enseignement supérieur et de la recherche, notamment les étudiants, des personnes dites « hébergées »[1] ou « invitées »[2] et des personnes utilisant ces moyens à raison d'un contrat passé avec l'université.

Article 4 – Les réseaux extérieurs

Par l'intermédiaire du réseau de l'établissement, les utilisateurs ont accès à des réseaux extérieurs : réseau régional SYVIK, réseau national RENATER et internet.

Les dispositions de la présente charte s'appliquent aux réseaux SYVIK et internet.

Par ailleurs, l'utilisation du réseau RENATER est régie par une charte déontologique que l'université s'est engagée à respecter et à faire respecter par l'ensemble des utilisateurs.

Chapitre 2 - Conditions et règles d'utilisation du système d'information et des technologies de l'information et de communication

Article 5 – Utilisation liée à l'activité de service public et utilisation privée

En ce qui concerne les utilisateurs personnes physiques telles qu'énoncées à l'article 3, la distinction suivante doit être opérée entre :

- l'utilisation du SI et des TIC relevant de l'activité de service public de l'enseignement supérieur et de la recherche ;
- l'utilisation à titre privé qui est autorisée sous réserve d'être non lucrative, raisonnable dans la fréquence et la durée et de ne pas nuire à la qualité et au fonctionnement du service. Par ailleurs, l'université veille à ce qu'il n'y ait pas d'utilisation abusive du SI et des TIC à ce titre.

[1] Les personnes hébergées sont les personnes présentes dans les bases de gestion des ressources humaines de l'établissement mais non payées par l'établissement.

[2] Les personnes invitées sont les personnes ne figurant dans aucune base de gestion des ressources humaines ou autre base métier de l'établissement.

Toute information est réputée liée à l'activité de service public 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 éventuel de ses données à caractère privé dans un espace prévu explicitement à cet effet (espace dénommé « privé ») dont la responsabilité et la sauvegarde lui incombent.
En cas de départ définitif de l'établissement, il appartient à l'utilisateur de détruire ses données à caractère privé.
L'utilisateur est seul responsable de l'usage qu'il fait des ressources informatiques, réseaux, services numériques et accès internet mis à disposition.

Article 6 – Respect de la vie privée
Le respect de la vie privée est garanti par la loi.
La jurisprudence a défini les conditions dans lesquelles un contrôle de l'usage du SI et des TIC peut être instauré.
L'utilisateur est informé de l'existence de procédures de surveillance, de contrôle et d'archivage mises en œuvre pour des raisons de sécurité des systèmes d'information, notamment pour l'utilisation de la messagerie électronique et d'internet tels que mentionné à l'article 19 de la présente charte.
L'utilisateur est informé que l'université de Caen conserve les données relatives à l'utilisation du système d'information conformément aux dispositions du code des postes et télécommunication et notamment son article L34-1.

Par ailleurs, l'utilisateur ne doit faire usage d'aucune image ou information relative à la vie privée d'autrui, ni les diffuser, sans son consentement.

Article 7 – Respect du secret de la correspondance
Le fait d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie de communications électroniques peut faire l'objet de sanctions pénales[3].

Article 8 – Respect de la propriété intellectuelle
Les utilisateurs du SI et des TIC doivent respecter les dispositions du code de la propriété intellectuelle[4].
L'utilisateur doit notamment :
- 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 sans avoir obtenu l'autorisation du ou des titulaire(s) des droits (les logiciels et documents « libres » relèvent aussi de ces dispositions).
De la même façon les marques ne peuvent être utilisées sans autorisation du ou des propriétaire(s)[5].

Article 9 – Respect des dispositions du Règlement Général sur la Protection des Données (RGPD EU2016/679)
Le Règlement Général sur la Protection des Données (RGPD 2016EU/679) a créé un dispositif juridique pour encadrer la mise en œuvre des « traitements automatisés de données à caractère personnel et des traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers ».
Les données à caractère personnel sont des informations qui permettent directement ou indirectement l'identification des personnes physiques auxquelles elles s'appliquent.
L'utilisateur doit donc avant toute création de fichier ou collecte de données comprenant ce type d'information, y compris lorsqu'elle résulte d'interconnexions de fichiers existants ou relative à un exercice pédagogique, saisir le Délégué à la Protection des Données de l'établissement à l'adresse dpo@unicaen.fr ou par téléphone au 02-31-56-50-20 et se conformer à ses préconisations.
Par ailleurs, la loi ouvre aux personnes un droit d'accès, de rectification, de suppression et de limitation sur les données les concernant. Ce droit s'exerce à l'UNICAEN auprès du Délégué à la Protection des Données.

Article 10 – Responsabilité en matière de transmission d'informations
L'utilisateur ne doit pas diffuser des informations ou données dont le contenu présente un caractère illégal ou pouvant porter atteinte à la dignité d'autrui, atteinte à l'image ou formulant des propos racistes, diffamatoires, injurieux, malveillants, menaçants, calomnieux, heurtant la sensibilité d'un tiers, de dénigrement, portant atteinte à la vie privée, ou violant le secret professionnel.
L'utilisateur s'engage à ne pas nuire à l'université ou à sa réputation.
La diffusion d'information d'ordre syndicale est autorisé sur les listes dédiées à cet effet.

Ceci s'applique tant aux fichiers qu'aux messages avec ou sans pièces attachées, quelle que soit la forme des contenus (textuels, sonores, audiovisuels ou multimédias).

[3] article 226-15 du code pénal
[4] voir notamment les articles L.111-1 et L.112-2
[5] article L.711-1

Article 11 – Respect des contrats passés par l'université
L'université offre certaines ressources électroniques (documentaires, pédagogiques...) résultant de contrats passés avec des prestataires extérieurs. L'utilisateur doit respecter les clauses contractuelles liant l'établissement avec ces prestataires.

Article 12 – Communications électroniques
Les Moyens de Communication par Voie Électronique (MCVE) recouvrent notamment le web, la messagerie, la messagerie instantanée, les forums, la téléphonie par internet, les espaces de travail collaboratif et toute forme d'accès à internet.

L'utilisateur doit veiller notamment à ce que la diffusion des informations soit limitée aux seuls destinataires concernés afin d'éviter la diffusion des informations en masse, l'encombrement inutile des MCVE et une dégradation du service.
Pour préserver le bon fonctionnement des services et des réseaux, l'université peut mettre en place des limitations concernant en particulier la taille des messages et des boîtes aux lettres.

L'utilisateur est informé que la consultation ou la participation à des sites illégaux (incitation la haine raciale, négationnisme, incitation à la violence, apologie du terrorisme…), sans motif légitime, est strictement interdite.

D'une manière générale, l'utilisateur est informé des risques et limites inhérents à l'usage des MCVE, en ce qui concerne notamment les défauts de sécurité dans la transmission des données et la fiabilité des informations disponibles sur le réseau.

Article 13 – Valeur juridique d'un message électronique
L'utilisateur est informé qu'un message électronique peut constituer une preuve ou un commencement de preuve susceptible d'engager la responsabilité de l'établissement ou la sienne.
En effet, la loi[6] reconnaît une valeur juridique à l'écrit sous forme électronique. Il en est ainsi, notamment, des contrats sous forme électronique.
L'utilisateur doit donc être vigilant sur la nature des écrits électroniques au même titre que pour les écrits traditionnels.

Article 14 – Continuité du service et interopérabilité
Afin d'assurer la continuité du service, les personnels doivent garantir à tout moment l'accès à leurs données professionnelles et doivent notamment, dans le cadre des activités liées au service, utiliser les espaces protégés et sauvegardés mis à leur disposition pour le stockage des données.
En cas d'absence, toute mesure visant à garantir la continuité du service public assuré par l'UNICAEN peut être prise par les autorités hiérarchiques de l'université.
Par ailleurs, dans l'objectif d'assurer l'interopérabilité et la pérennité des données ainsi que la continuité du service, l'utilisation de formats ouverts de document et de stockage de l'information doit être privilégiée par l'utilisateur et facilitée par l'UNICAEN.

Chapitre 3 - Protection et sécurité

Article 15 - Protection
La protection des systèmes d'information s'appuie sur des dispositions légales[7] qui prévoient que sont interdits :
- l'accès illicite, c'est-à-dire toute introduction dans un SI par une personne non autorisée ;
- le maintien frauduleux, c'est-à-dire le maintien sur un SI après un accès illicite et après avoir pris conscience du caractère illicite de cet accès ;
- l'entrave au système, c'est à dire toute perturbation volontaire du fonctionnement d'un SI ;
- l'altération des données, c'est-à-dire toute suppression, modification, ou introduction de données « pirates » avec la volonté de modifier l'état du système informatique les exploitant ;
- le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions décrites ci-dessus.

Article 16 – Mesures de sécurité prises par l'établissement
Au titre de la sécurité du SI et des TIC, l'université prend les mesures suivantes :
- elle définit le niveau d'accès de chaque utilisateur en fonction de son profil qui est établi en prenant en compte son statut, sa fonction, la nature de ses activités et ses besoins ;
- elle limite pour chaque utilisateur l'accès aux ressources en fonction du niveau d'accès qui lui a été attribué ;

[6] articles 1316, 1316-4 et 1369-1 du code civil
[7] articles 323-1 et suivants du code pénal

- elle veille à ce que certaines ressources ne soient accessibles qu'aux personnes spécialement habilitées à cet effet ;
- elle définit la politique de gestion, d'audit et de renouvellement des mots de passe ;
- elle informe chaque utilisateur des règles et bonnes pratiques pour un usage sécurisé des ressources informatiques.

L'université s'engage à mettre en place toutes les procédures nécessaires afin de garantir le fonctionnement et la disponibilité des services et équipements mis à disposition.

Par ailleurs, l'université peut interrompre, modifier ou supprimer tout ou partie des services et équipements, de manière temporaire ou définitive.

Article 17 – Règles de sécurité que l'utilisateur doit respecter

Au titre de la sécurité du SI et des TIC, l'utilisateur doit respecter les prescriptions suivantes :
- garder strictement confidentiels son ou ses moyens d'accès au système d'information (mots de passe, carte professionnelle, carte étudiant, badge, ...). Tout utilisateur doit être enregistré dans les bases de référence de l'établissement et avoir obtenu des moyens d'accès qui lui sont personnels et confidentiels ; si, pour quelque raison que ce soit, l'utilisateur est informé ou estime qu'un ou plusieurs de ses moyens d'accès ne sont plus confidentiels, il doit procéder dès que possible au changement de ces derniers ou en demander la modification au responsable du dispositif ;
- s'engager à ce que ses mots de passe soient conformes aux préconisations de l'établissement ;
- ne pas utiliser les moyens d'accès d'un autre utilisateur, ni chercher à les connaître ou à se les approprier ;
- ne pas accéder ou tenter d'accéder à des ressources du SI et aux communications entre tiers pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des informations confidentielles ou des données dont le contenu serait contraire à la législation en vigueur ;
- ne pas connecter au SI des matériels autres que ceux autorisés par l'établissement ;
- ne pas installer, télécharger ou utiliser sur le SI des logiciels dont les droits de licence n'ont pas été acquittés ;
- ne pas apporter de perturbations au bon fonctionnement du SI et du réseau par des manipulations anormales de matériel ou par l'introduction de logiciels parasites ;
- ne pas quitter son poste de travail ou un poste en libre-service en laissant des ressources ou services accessibles.

Article 18 – Obligations d'information

L'UNICAEN porte à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du SI et des TIC.
L'utilisateur doit informer, sans délai, sa hiérarchie de tout dysfonctionnement constaté ou de toute anomalie constatée (intrusion, altération, destruction).
Il est également tenu de signaler au Responsable de la Sécurité des Systèmes d'Information (RSSI), nommé par le président de l'université, toute possibilité d'accès à une ressource qu'il aurait constatée et qui ne correspondrait pas à son habilitation.
Par ailleurs, la loi[8] impose que : « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au Procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».

Article 19 – Dispositions relatives à la maintenance et au contrôle

Pour assurer les opérations nécessaires de maintenance technique (corrective, évolutive ou préventive) la Direction du Système d'Information de l'université (DSI) et ses correspondants peuvent réaliser des interventions, éventuellement à distance, sur les moyens informatiques et de communication électronique mis à disposition de l'utilisateur.

Toute information bloquante ou présentant une difficulté d'acheminement à son destinataire peut être isolée, voire supprimée si nécessaire.
Dans le respect des dispositions légales et réglementaires, une surveillance et un contrôle de l'usage du SI et des TIC peuvent être mis en place à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.
Les personnels chargés des opérations de maintenance et de contrôle sont soumis à une obligation de confidentialité, ils doivent respecter la vie privée et le secret de la correspondance des utilisateurs sous la réserve de l'obligation légale citée dans l'article 18.

Chapitre 4 – Dispositions finales

[8] article 40 du code de procédure pénale

Article 20 – Sanction du non respect des dispositions de la charte

En cas de non respect des dispositions de la présente charte le président de l'université peut prendre toutes mesures conservatoires à l'encontre d'un utilisateur sans préjudice d'éventuelles procédures disciplinaires ou pénales qui seraient engagées.

Article 21 – Entrée en vigueur de la charte

La présente charte a été adoptée par le Conseil d'Administration de l'Université le 15 mai 2009 et modifiée par le Conseil le 22 juin 2018. Elle est annexée au règlement intérieur de l'Université de Caen Normandie.