La Rochelle Université

D'ici, on voit +loin !

RÈGLEMENT INTÉRIEUR DE L'USAGE DU SYSTÈME D'INFORMATION

univ-larochelle.fr

Sommaire

Préambule

Afin de respecter l'égalité entre les femmes et les hommes, le présent règlement intérieur est rédigé selon les principes de la rédaction égalitaire. Notamment, les accords en genre obéissent à la règle de proximité ou du sens, et non pas à la règle selon laquelle « le masculin l'emporte sur le féminin ».

Présentation

La Rochelle Université met en œuvre un système d'information et de communication nécessaire à l'exercice de ses missions. Elle met ainsi à disposition des personnels, des usagères et usagers et des autres utilisatrices et utilisateurs des outils informatiques, services numériques et des moyens de communication.

Le présent règlement définit les conditions d'accès et les règles d'utilisation de ces outils informatiques, services numériques et des moyens de communication de l'université. Il a également pour objet de sensibiliser les utilisatrices et les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'une utilisatrice ou d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'établissement.

Le règlement est diffusé à l'ensemble des utilisatrices et utilisateurs par tout moyen et à chaque modification. À ce titre, il est disponible sur le site Internet institutionnel de l'université. Il est systématiquement communiqué à tout nouvel arrivant ou arrivante. Des actions de communication internes sont organisées régulièrement afin d'informer les utilisatrices et utilisateurs des pratiques recommandées.

Définitions

Catalogue des services numériques[1] : ensemble des services numériques mis à disposition par l'établissement.

Délégué·e à la protection des données (DPO)[2] : personne chargée de la protection des données au sein d'une organisation.

Donnée à caractère personnel : toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Une personne est identifiée lorsque son nom apparaît dans un fichier. Une personne est identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification : adresses postales et électroniques (courriel) ; IP (identification de la machine utilisée) ; numéro d'immatriculation ou de compte bancaire, identifiants de connexion, numéro de téléphone, numéro de sécurité sociale ; photographie ; voix ; données de localisation…

Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès la ou le responsable du traitement ou toute autre personne.

Une donnée à caractère personnel peut donc aussi être une donnée professionnelle.

Direction du système d'information (DSI) : service responsable du système d'information de l'établissement. La DSI met en œuvre la politique des systèmes d'information, des technologies de l'information et de la communication définie par la présidente ou le président et le conseil d'administration dans les domaines de l'enseignement, de la gestion, de la recherche, de la documentation et du pilotage de l'établissement.

1 https://services-numeriques.univ-larochelle.fr/Catalogue-des-services
2 Pour contacter la ou le délégué à la protection des données : dpo@univ-lr.fr

Environnement numérique de travail (ENT)[3] : portail rassemblant, en un point d'accès unique, les ressources et services numériques mis à disposition des utilisatrices et utilisateurs en fonction de leur profil.

Équipements nomades : tous les moyens techniques mobiles (ordinateur portable, imprimante portable, tablette, téléphone mobile ou smartphone, objet connecté, CD ROM, clé USB, disque dur amovible, etc.).

Informations d'authentification : identifiant, mot de passe, code pin, clés privées, etc.

Information professionnelle : information utilisée en contexte de travail. Sa sensibilité est qualifiée selon quatre critères (publique, interne, confidentielle, secrète).

Mention « Privé » : par défaut, toute ressource (document, dossier, courriel,…) est considérée comme étant de nature "professionnelle" (pour les personnels) ou "universitaire" (pour les autres utilisatrices et utilisateurs). Il revient donc à l'utilisatrice ou l'utilisateur de clairement identifier, le cas échéant, celles relevant de sa vie privée en apposant la mention « Privé·e », « Personnel·le » et/ou « Private ». Les ressources identifiées comme telles (ainsi que leur contenu dans le cas d'un dossier) ne pourront alors être consultées qu'avec l'accord de l'utilisatrice ou l'utilisateur ou sur décision de justice. Attention : La mention « Privé » ne sera pas considérée comme valable si elle est utilisée au niveau du nom d'une partition d'un disque dur ou d'une clé USB (il faut – dans ce cas – ajouter un dossier avec la mention « Privé » à la racine).

À noter enfin que les intitulés suivants ne permettent pas de considérer la ressource comme étant privée :

> les nom(s) et/ou prénom(s) et/ou initiales de la personne ;

> les dénominations « Mes documents », « Mes images »,… et leurs dérivés.

Outils informatiques : tous les équipements matériels et logiciels informatiques et de reprographie de l'université.

Services numériques : ensemble des services offerts aux utilisatrices et utilisateurs via les applications ayant accès au système d'information de l'établissement. Les services numériques de l'université sont généralement accessibles via l'ENT.

Moyens de communication : les supports de diffusion d'informations, comme internet, la messagerie électronique, les réseaux sociaux, les forums et toutes les nouvelles technologies de l'information et de la communication.

Règlement général sur la protection des données (RGPD) : règlement européen (UE) 2016/679 du 27 avril 2016 et mise en application le 25 mai 2018, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE.

Responsable de la sécurité du système d'information (RSSI)[4] : personne chargée de la sécurité du système d'information. Elle est nommée par la présidente ou le président de l'université.

Sécurité physique : sécurité concernant tous les aspects liés à l'environnement dans lequel les systèmes se trouvent.

Sécurité logique : sécurité faisant référence à la réalisation de mécanismes techniques de sécurité par logiciel.

Site malveillant : tout site Web conçu pour faire accomplir à une utilisatrice ou un utilisateur légitime des actions indésirables ou néfastes pour la sécurité du système d'information.

Structure : entité administrative ou d'enseignement ou de recherche rattachée à l'établissement (services centraux, communs ou inter-universitaires ; composantes ; instituts ; écoles doctorales ; unités de recherches propres ou mixtes dont la tutelle principale est l'université).

3 https://ent.univ-lr.fr
4 Pour contacter la ou le responsable de la sécurité du système d'information : rssi@univ-lr.fr

Système d'information (SI) : ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications mis à disposition par l'université.

Tiers : une application, une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, la personne responsable du traitement, la personne sous-traitante et les personnes qui, placés sous l'autorité directe de la personne responsable du traitement ou de la personne sous-traitante, sont autorisées à traiter les données à caractère personnel – Règlement (UE) 2016/679 du 27 avril 2016.

Traitements de données : opérations informatisées portant sur des données telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Utilisatrice ou utilisateur : toute personne autorisée à accéder et à utiliser les outils informatiques et moyens de communication de l'université (agentes et agents titulaires ou contractuels, usagères et usagers, intervenantes et intervenants extérieurs, visiteurs et visiteuses, invité·es, etc.).

Usagère et usager : toute personne bénéficiaire du service public de l'enseignement supérieur. La catégorie "usagère et usager" comprend les étudiantes et étudiants, qu'ils soient inscrits en formation initiale ou en formation continue, et les auditeurs et auditrices libres. Les doctorantes et doctorants relèvent des règles relatives aux personnels dans le présent règlement.

Article I. Champ d'application

Le présent règlement s'applique à toute utilisatrice et tout utilisateur du système d'information et de communication de l'université quelles que soient ses activités.

Les usages relevant de l'activité des organisations syndicales sont régis par une charte conforme au décret n° 82-447 du 28 mai 1982 relatif à l'exercice du droit syndical dans la fonction publique et la décision ministérielle du 24 mai 2016 relative aux conditions et aux modalités d'utilisation des technologies de l'information et de la communication par les organisations syndicales[5].

Article II. Conditions d'utilisation du système d'information

Chaque utilisatrice et utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle ou universitaire dans les conditions définies par l'université.

L'utilisatrice ou l'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie[6]. En tout état de cause, l'utilisatrice ou l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

II.1. Utilisation "universitaire" / privée

Le système d'information est composé d'outils de travail ouverts à des usages universitaires, professionnels, administratifs, pédagogiques et de recherche et peuvent aussi constituer le support d'une communication privée.

L'usage des ressources est réservé à l'activité professionnelle pour les personnels et à la réalisation de travaux liés à l'exercice des missions de l'université pour les autres utilisatrices et utilisateurs.

Toute information traitée dans ce cadre est réputée "professionnelle" pour les personnels et "universitaire" pour les autres utilisatrices et utilisateurs à l'exclusion des données explicitement désignées par l'utilisatrice ou l'utilisateur comme relevant de sa vie privée. Il appartient à l'utilisatrice ou l'utilisateur de procéder au stockage et à la sauvegarde de ces dernières dans un dossier intitulé « Privé ». En tout état de cause, les données non situées

5 NOR : MENH1610318S
6 Par exemple le secret médical dans le domaine de la santé.

dans un répertoire « Privé » sont considérées comme des données appartenant à l'établissement qui pourra en disposer.

L'utilisation du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. L'espace utilisé ne doit pas occuper une part excessive des ressources. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisatrice ou l'utilisateur, au temps qu'il y consacre et au bon fonctionnement de l'établissement.

L'utilisation des ressources du système d'information à titre privé doit respecter la réglementation en vigueur. Sont notamment interdits le téléchargement illégal, la détention, la diffusion et l'exportation d'images à caractère pédophile, la diffusion de contenus à caractère raciste ou antisémite, la diffusion de messages contraires à la décence et l'enregistrement ou la diffusion d'images de violence.

Cas particulier de l'utilisation de ressources informatiques personnelles : l'utilisation de ressources informatiques personnelles (ordinateurs, smartphones, tablettes, etc. achetés sur des fonds personnels), lorsque celles-ci sont utilisées pour accéder localement ou à distance aux ressources de l'université, ne doit pas remettre en cause ou affaiblir les politiques de sécurité en vigueur par une protection insuffisante ou une utilisation inappropriée. Ces ressources personnelles doivent être conformes aux règles de sécurité édictées dans le présent règlement.

Les données professionnelles sont la propriété de l'université. Elles ne doivent pas être enregistrées ou stockées sur les ressources informatiques personnelles ou sur des plateformes opérées par des tiers non autorisés. En outre, afin d'assurer la continuité du service en cas d'absence, il est interdit de placer dans un espace privé toute information de nature professionnelle.

II.2. Continuité de service : gestion des absences et des départs des personnels

Lors de son départ ou d'une absence prolongée, l'utilisatrice ou l'utilisateur doit remettre tous les documents professionnels (administratifs, recherche et pédagogiques…) à sa ou son responsable de structure ou lui permettre d'y accéder.

En cas d'indisponibilité de l'utilisatrice ou l'utilisateur, sa ou son responsable de structure peut demander à la DSI d'accéder à tous les documents et informations professionnels (hors dossier « Privé »).

Les comptes et les données rattachées (qu'elles soient professionnelles ou identifiées comme « privées ») de l'utilisatrice ou l'utilisateur sont supprimés dans un délai maximum de 12 mois à compter de la date de son départ. Ce délai est accordé pour permettre à l'utilisatrice ou l'utilisateur de régulariser sa situation (nouveau contrat, convention, réinscription) et de récupérer ses données (ou de transmettre les données à ses ayants-droits).

L'utilisatrice ou l'utilisateur est responsable de la récupération des données stockées dans son dossier « Privé ». La responsabilité de l'établissement ne peut être engagée quant à la conservation de ces données.

L'utilisatrice ou l'utilisateur doit restituer à la DSI, les matériels (ordinateurs portables, téléphones, disques durs externes, clés USB…) mis à sa disposition par l'établissement.

Le compte informatique d'une personne est lié à la présence ou à l'activité de celle-ci au sein de l'université. La période de validité des comptes est donc calculée en fonction du statut de l'utilisatrice ou l'utilisateur. Un délai est accordé à l'utilisatrice ou l'utilisateur après son « départ » (fin d'études, de contrat, de convention, démission…) afin de lui permettre de régulariser sa situation à l'université (réinscription, signature d'un nouveau contrat…) et de préparer ledit départ (transfert de ses dossiers à ses collègues ou sa hiérarchie, sauvegarde de ses données à caractère privé, envoi de messages à ses collègues pour les alerter du changement d'adresse électronique, etc.). Ce délai varie en fonction du statut de l'utilisatrice ou l'utilisateur (étudiante ou étudiant, personnel, chercheuse ou chercheur

invité, personne extérieure à l'établissement, etc.) et ne peut en aucun cas dépasser les 90 jours.

Article III. Principes de sécurité

Les principes suivants ont pour objectif de protéger les informations qui constituent le patrimoine immatériel de l'université contre toute altération, volontaire ou accidentelle, de leur confidentialité, intégrité ou disponibilité. Tout manquement aux règles qui régissent la sécurité du système d'information est en effet susceptible d'avoir des impacts importants (humains, financiers, juridiques, environnementaux, atteintes au fonctionnement de l'organisme, au potentiel scientifique et technique ou à la vie privée).

III.1. Règles de sécurité applicables

L'université met en œuvre les mécanismes de protection adaptés sur le système d'information mis à la disposition des utilisatrices et utilisateurs.

L'utilisatrice ou l'utilisateur est informé que les informations d'authentification qui lui sont attribuées constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive.

Les niveaux d'accès au système d'information ouverts à l'utilisatrice ou l'utilisateur sont définis en fonction des missions qui lui sont confiées. Il est responsable de l'utilisation du système d'information auquel il accède avec les droits qui lui sont conférés par sa ou son responsable de structure. En cas d'évolution de ses missions, les autorisations sont modifiées par la ou le responsable de structure. La sécurité des ressources mises à la disposition de l'utilisatrice ou l'utilisateur lui impose le respect des règles suivantes :

> de la part de l'université :

- > Limiter l'accès aux seules ressources pour lesquelles l'utilisatrice ou l'utilisateur est expressément autorisé ;
- > Garantir la disponibilité, l'intégrité et la confidentialité des données de l'utilisatrice ou l'utilisateur.

> de la part de l'utilisatrice ou de l'utilisateur :

- > Se conformer aux directives de sécurité concernant les usages…
  - … relatifs à la connexion :
    - appliquer la politique de gestion des mots de passe de l'université ;
    - garder strictement confidentiel ses informations d'authentification ;
    - ne pas utiliser les informations d'authentification d'une autre utilisatrice ou d'un autre utilisateur, ni chercher à les connaître ;
    - ne pas enregistrer ses informations d'authentification sur des applications ou espaces non maîtrisés par l'université ;
    - ne pas masquer sa véritable identité, ne pas usurper l'identité d'autrui, ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas, s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'autorisation explicite ;
    - ne pas se connecter délibérément à des sites Internet malveillants ;
    - s'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations du matériel ou du logiciel ;
    - verrouiller ou fermer toutes les sessions en cours sur son poste de travail, en cas d'absence, même momentanée ;
    - s'assurer que toute personne externe susceptible d'accéder au système d'information de l'université y est autorisée par la ou le responsable de structure. Cette autorisation comprend l'engagement de respecter le présent règlement.

- … relatifs aux données et documents professionnels :
  - protéger les informations que l'utilisatrice ou l'utilisateur est habilité à manipuler dans le cadre de ses fonctions, selon leur sensibilité. Lorsqu'elle crée un document, l'utilisatrice ou 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.) ;
  - n'opérer les sauvegardes de données, les partages d'information, les échanges collaboratifs, que sur des sites hébergés ou faisant l'objet d'une convention signée par l'université et dont la sécurité a été vérifiée par celle-ci ;
  - ne pas utiliser des supports de données tels que les ordinateurs, clés USB, CDROM, DVD,… ou tous autres périphériques externes ou plateformes opérées par des tiers (cloud, etc.) sans respecter les règles de sécurité de l'université et prendre les précautions nécessaires pour s'assurer de leur innocuité ;
  - respecter les règles définies par l'université, obtenir l'autorisation de sa ou son responsable de structure pour tout traitement de données réalisé sur un support externe ;
  - mettre en œuvre un système de sauvegarde manuel lorsque des sauvegardes automatiques ne sont pas prévues ;
  - s'assurer que son poste de travail est verrouillé ou que la session est fermée lors d'une absence même momentanée de son bureau afin de se prémunir contre les risques de vol ou suppression de documents sensibles ;
  - s'assurer que les dispositions contractuelles avec des intervenantes et intervenants extérieurs comportent les clauses rappelant les rôles et les obligations des personnes concernant la gestion et la sécurisation des données et documents professionnels.

> Respecter les consignes de sécurité concernant le matériel ou les logiciels :

- ne pas modifier les paramétrages de sécurité du poste de travail ;
- ne pas installer, télécharger ou utiliser des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites de confiance, ou sans autorisation de sa ou son responsable de structure ;
- ne pas copier, modifier, détruire les logiciels propriétés de l'université ;
- respecter les dispositifs mis en place par l'université pour lutter contre les virus et les attaques par programmes informatiques ;
- utiliser les moyens de protection mis à disposition contre le vol (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 contiennent (ordinateur portable, disque dur, clé USB, smartphones, tablettes, etc.) ;
- ne pas désactiver, ni altérer le fonctionnement ou désinstaller l'outil de cryptage lorsqu'il a été installé par l'université ;
- adapter la sécurité (physique et logique) des équipements nomades en fonction de la sensibilité de l'information qu'ils traitent et stockent, conformément aux recommandations de l'Agence nationale de la sécurité des systèmes d'information[7] ;
- lors de déplacements, en particulier à l'étranger, privilégier l'utilisation d'équipements dédiés (ordinateur compris) ne contenant que les données nécessaires et suffisantes au bon déroulement de sa mission, conformément aux recommandations de l'Agence nationale de la sécurité des systèmes d'information. Cette recommandation devient obligatoire lorsque l'utilisatrice ou

7 https://www.ssi.gouv.fr/

l'utilisateur se déplace dans un pays « à risque »[8] et que son équipement habituel contient des données sensibles.

> Signaler le plus rapidement possible à la ou au responsable de la sécurité du système d'information tout logiciel ou dispositif suspect ainsi que toute perte, tout vol ou toute compromission suspectée ou avérée :
  - d'un équipement stockant des données professionnelles ;
  - de ses informations d'authentification (identifiant, mot de passe, code pin, clés privées, etc.).

III.2. Mesures de contrôle de la sécurité

L'utilisatrice ou l'utilisateur est informé que :

> l'université peut intervenir (y compris à distance) sur les ressources mises à sa disposition pour effectuer une maintenance corrective, curative ou évolutive ;

> toute information bloquante ou générant une difficulté technique pour le système doit être isolée et/ou supprimée ;

> des systèmes automatiques de filtrage permettant de diminuer les flux d'information et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Ce filtrage peut être neutralisé sur autorisation de la ou du responsable de structure pour des raisons uniquement professionnelles ;

> la DSI dispose d'outils techniques pour procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place ;

> en cas d'irrégularité ou de suspicion/découverte d'activités suspectes, la DSI peut être amenée – sans notification préalable – à suspendre le compte informatique d'une utilisatrice ou d'un utilisateur, à en limiter ses droits ou encore à bloquer l'usage de certains équipements sur le réseau de l'université.

Article IV. Moyens de communication

IV.1. Messagerie électronique

L'utilisation de la messagerie constitue un élément essentiel d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'université.

Adresses électroniques

Sauf cas particulier, l'université met à la disposition de l'utilisatrice ou de l'utilisateur une adresse électronique nominative lui permettant d'émettre et de recevoir des messages. L'utilisation de cette adresse électronique dite « institutionnelle » ou « professionnelle » relève de la responsabilité de la personne qui la détient. Son utilisation est interdite sur des sites sans rapport avec son activité à l'université. L'aspect nominatif de l'adresse électronique ne retire en rien le caractère institutionnel de la messagerie.

Une adresse électronique fonctionnelle ou organisationnelle, dite « alias », peut être mise en place pour une utilisatrice ou un utilisateur ou un groupe d'utilisatrices et d'utilisateurs pour les besoins de l'université.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'utilisatrices et d'utilisateurs, relève de la responsabilité exclusive de l'université : ces listes ne peuvent être utilisées sans autorisation explicite et sont soumises à modération préalable.

Contenu des messages électroniques

Tout message reçu ou émis via l'adresse institutionnelle est réputé professionnel.

Les messages à caractère personnel sont tolérés, ils doivent être signalés par la mention « [Privé] » dans leur objet et être classés dès l'envoi dans un dossier nommé « Privé ».

8 https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/conseils-par-pays-destination/

De même, les messages reçus, lorsqu'ils sont à caractère personnel, doivent être classés dans un dossier nommé « Privé ». Il est recommandé d'utiliser sa messagerie personnelle pour l'envoi et la réception de messages présumés à caractère personnel.

Un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de limiter l'envoi de messages non sollicités afin de ne pas engager la responsabilité civile ou pénale de l'université et de l'utilisatrice ou l'utilisateur. Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature ; il s'agit notamment des contenus portant atteinte à la vie privée d'autrui (par exemple : diffamation, injure, menace, atteinte à la propriété intellectuelle…).

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, en application des dispositions du code civil. L'utilisatrice ou l'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels. Le courriel est un document administratif reconnu en tant que preuve en cas de contentieux.

Émission et réception des messages

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

Les messages électroniques envoyés font l'objet d'un contrôle automatique antiviral. Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération lors d'envoi de correspondances importantes. La transmission de données confidentielles par messagerie électronique est interdite sauf utilisation d'un dispositif de cryptage validé par la DSI.

Les messages électroniques reçus font l'objet d'un contrôle automatique antiviral et anti-spam. L'utilisatrice ou l'utilisateur doit faire preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, hameçonnage…).

Afin de préserver le bon fonctionnement du service de messagerie, la transmission de messages électroniques n'est possible que vers un nombre limité de destinataires. Cette limite peut être levée par l'utilisation de listes de diffusion ouvertes sur demande auprès de la DSI. De même, la taille, le nombre et le type des pièces jointes peuvent être limités pour éviter l'engorgement ou la dégradation du système de messagerie. Il est recommandé d'utiliser la solution d'envoi de gros fichiers proposée dans l'ENT par la DSI.

La capacité de stockage des messages électroniques est limitée. L'utilisatrice ou l'utilisateur doit de ce fait régulièrement supprimer ses messages. S'il souhaite les conserver, il lui appartient de les archiver.

La redirection automatique des messages vers une boîte de messagerie alternative n'est autorisée que si cette dernière est opérée par un tiers de confiance (CNRS, autre université, etc) et uniquement pour une période déterminée. Pour que cette redirection soit mise en place, l'utilisatrice ou l'utilisateur doit en faire la demande auprès de la DSI, qui pourra la refuser si toutes les conditions ne sont pas respectées.

IV.2. Internet

L'établissement est signataire de la charte RENATER (Réseau national de télécommunications pour la technologie l'enseignement et la recherche)[9]. Dans ce cadre, il se doit de faire respecter les règles déontologiques qui y sont décrites.

Par ailleurs, il est rappelé qu'Internet est soumis au respect de l'ensemble des règles de droit en vigueur.

L'outil Internet mis à disposition permet de consulter tous types de sites présentant un lien direct et nécessaire avec l'activité professionnelle ou estudiantine de l'utilisatrice ou l'utilisateur. Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, de sites Internet dont le contenu n'est pas contraire à la loi et à l'ordre public et ne mettant pas en cause l'intérêt et la réputation de l'établissement, est admise.

9 https://www.renater.fr/IMG/pdf/charte_fr.pdf

L'Université se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités. Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'université. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou l'établissement.

L'utilisatrice ou l'utilisateur doit adopter un comportement loyal vis-à-vis de l'université lors de l'utilisation des réseaux sociaux, des blogs, qu'ils soient professionnels ou non.

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

Seuls les « clouds » présentés dans le catalogue des services numériques[10] de l'établissement et dont les règles de sécurité sont maîtrisées et validées par l'université peuvent être utilisés pour le dépôt de données professionnelles. Ceci exclut de facto les « clouds » personnels de type Google Drive, Dropbox, iCloud, OneDrive, etc.

IV.3. Téléchargements

Le téléchargement de logiciels ou d'œuvres protégées doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article VII du présent règlement. Il doit être fait dans le cadre d'usages universitaires, professionnels, pédagogiques ou liés à la recherche.

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

IV.4. Publication sur les sites Internet de l'université

La présidente ou le président de l'université, en tant que représentant légal de l'université, est le directeur de publication de l'établissement pour les sites Internet mis en œuvre par l'établissement. Toute publication de pages d'information sur les sites Internet de l'université doit être conforme à la politique Internet de l'établissement et validée par une ou un responsable de publication désigné.

Préalablement à un projet de diffusion d'informations relatives à des personnes sur un site Internet, le service doit prendre attache auprès de la ou du délégué à la protection des données (cf. article VIII).

Aucune publication de pages d'information à caractère privé n'est autorisée sur les ressources du système d'information de l'université, sauf cas particulier autorisé par la présidente ou le président.

Chaque site rattaché au nom de domaine de l'établissement doit comporter les mentions légales obligatoires et pointer également sur la rubrique dédiée « mentions légales » du site de l'université.

Toute publication doit respecter la réglementation en vigueur et notamment celle relative à l'accessibilité.

Les informations publiées sur les sites du domaine de l'université doivent également être fiables et régulièrement mises à jour.

Article V. Traçabilité

L'Université informe l'utilisatrice ou l'utilisateur que le système d'information est surveillé et contrôlé dans le respect de la législation, à des fins de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité, de détection des abus et fraudes, notamment fraude aux examens, détournement de finalité des applicatifs de gestion, etc., ainsi qu'à des fins statistiques suivant la politique de gestion des traces de l'université.

Les services informatiques de l'université opèrent, sans avertissement, les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'un de ses composants. Ils s'appuient pour ce faire, sur des fichiers de journalisation, appelés

10 https://services-numeriques.univ-larochelle.fr/Catalogue-des-services

également « traces », « journaux » ou « logs », qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent au minimum les données suivantes : date, identifiant et type d'événement.

Ces fichiers de journalisation sont conservés au minimum 3 mois et au maximum 12 mois selon la réglementation applicable au type de données conservées.

Article VI. Confidentialité et protection des données à caractère personnel

Toute utilisatrice ou tout utilisateur autorisé à accéder aux données du système d'information de l'université s'engage à maintenir confidentielle l'information à laquelle il accède dans le cadre de ses fonctions. Les utilisatrices et utilisateurs autorisés à accéder à l'information du système d'information de l'université doivent être vigilants vis-à-vis des données auxquelles ils accèdent au sens de la politique de sécurité du système d'information.

L'utilisatrice ou l'utilisateur est responsable des fichiers et répertoires qu'il constitue. Il est cependant interdit de prendre connaissance d'informations détenues par d'autres utilisatrices et utilisateurs, quand bien même ceux-ci ne les auraient pas correctement protégées.

L'utilisatrice ou l'utilisateur ne doit pas tenter d'intercepter des communications entre tiers.

L'information collectée et contenue dans les fichiers et les bases de données exploitées par l'établissement a un caractère confidentiel. La manipulation et l'exploitation des données doivent être conformes au RGPD et aux dispositions consignées dans les déclarations à la CNIL.

Par conséquent, toute utilisatrice et tout utilisateur est tenu d'assurer la protection des données à caractère personnel qu'il traite dans le cadre de ses fonctions notamment en :

- limitant strictement aux besoins de son activité la diffusion par des moyens informatiques ou autre (impressions papier par exemple) des données à caractère personnel en sa possession ;
- protégeant les codes d'accès aux applications et systèmes d'information qu'il utilise ;
- ne conservant pas ces données au-delà de la durée nécessaire au traitement auquel elles sont destinées ;
- informant immédiatement sa hiérarchie, ou la ou le délégué à la protection des données, ou la ou le responsable de la sécurité du système d'information le cas échéant, si toute personne utilisatrice des outils informatiques, services numériques et des moyens de communication constatait un défaut dans la protection de données à caractère personnel ;
- sécurisant la communication de données à caractère personnel, afin que la confidentialité, l'intégrité et l'authenticité des informations soient assurées.
- impliquant la ou le délégué à la protection des données pour tout projet de transmission interne ou externe de données.

Tout traitement de données à caractère personnel, y compris la simple collecte, doit être analysé, étudié et répertorié dans le registre des traitements.

Article VII. Respect de la propriété intellectuelle

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

En conséquence, chaque utilisatrice et utilisateur doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Par ailleurs, l'usage des ressources documentaires doit être conforme au contrat de mise à disposition de l'éditeur validé par l'université. Notamment, le téléchargement massif et systématique de ressources documentaires par l'intermédiaire d'un robot ou de tout autre logiciel est interdit.

Article VIII. Respect de la loi informatique et libertés

L'utilisatrice ou l'utilisateur est tenu de respecter les dispositions légales en matière de traitement de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite « loi Informatique et Libertés ».

Toute création de fichiers comprenant des informations à caractère personnel et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « Informatique et Libertés » et le RGPD.

La ou le délégué à la protection des données de l'université doit donc être saisi préalablement à la mise en place de tout traitement de données afin de valider leur conformité avec le RGPD. Ce traitement fait l'objet d'une fiche qui est consignée dans le registre des traitements de l'établissement.

En outre, chaque utilisatrice et utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation du système d'information. Ce droit s'exerce auprès de la présidente ou du président de l'université, Technoforum – 23 avenue Albert Einstein – BP 33060 – 17031 La Rochelle. La ou le délégué à la protection des données est informé par transmission d'une copie de toute demande d'accès, de rectification et d'opposition à l'utilisation des données personnelles.

Article IX. Limitation des usages et sanctions

L'utilisatrice ou l'utilisateur est tenu de respecter l'ensemble des règles définies dans le présent règlement, ainsi que les textes de référence applicables annexés.

Tout manquement à ces règles et mesures de sécurité et de confidentialité est susceptible d'engager la responsabilité de l'utilisatrice ou l'utilisateur et d'entraîner à son encontre des sanctions disciplinaires et pénales en fonction de la gravité des faits constatés par les instances compétentes. L'établissement pourra, sans préjuger des procédures pouvant être engagées à l'encontre de l'utilisatrice ou l'utilisateur malveillant, délivrer un avertissement, limiter ou suspendre les usages par mesure conservatoire, sans préavis.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisatrice ou l'utilisateur à des fins extra-professionnelles est également passible de sanctions.

Article X. Entrée en vigueur

Le présent règlement annule et remplace tous documents relatifs à l'utilisation du système d'information de l'université.

Annexe – Principaux textes de référence applicables

> Règlement européen (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données – RGPD)

> Code civil

> Code pénal

> Code de la propriété intellectuelle

> Loi du 29 juillet 1881 sur la liberté de la presse

> Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

> Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

> Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

> Charte déontologique RENATER : https://www.renater.fr/IMG/pdf/charte_fr.pdf

> Dispositions relatives au respect de la vie privée, de l'ordre public, du secret professionnel

> Dispositions relatives à la protection du potentiel scientifique et technique de la nation : code pénal, code de la défense, arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation

La Rochelle Université

D'ici on voit + loin !

La Rochelle Université

23 avenue Albert Einstein
BP 33060
17031 La Rochelle

univ-larochelle.fr