



Charte régissant l'usage du
système d'information au sein
de l'Université de Reims
Champagne-Ardenne

SOMMAIRE

Préambule	3
Article I. Champ d'application.....	4
Article II. Conditions d'utilisation des systèmes d'information	4
Section II.1 Utilisation professionnelle / privée	4
Section II.2 Matériel personnel / professionnel.....	5
Section II.3 Outils de communication / Cloud computing	5
Section II.4 Continuité de service : gestion des absences et des départs.....	5
Section II.5 Droit à la déconnexion et l'usage de la messagerie à l'URCA.....	6
Article III. Principes de sécurité.....	6
Section III.1 Règles de sécurité applicables	6
Section III.2 Mesures de contrôle de la sécurité.....	7
Section III.3 Protection antivirale	8
Article IV. Numérique Responsable	8
Section IV.1 Sobriété énergétique.....	8
Section IV.2 Utilisation rationnelle des ressources.....	8
Section IV.3 Économie circulaire.....	9
Section IV.4 Communication numérique éco-responsable.....	9
Article V. Communication électronique	9
Section V.1 Messagerie électronique	9
(a) Adresses électroniques	9
(b) Contenu des messages électroniques	10
(c) Émission et réception des messages	10
(d) Statut et valeur juridique des messages.....	10
(e) Stockage et archivage des messages.....	10
(f) Gestion des absences	10
(g) Décès ou départ soudain de l'utilisateur.....	11
(h) Modalités d'accès à une boîte de messagerie.....	11
Section V.2 Internet.....	12
Section V.3 Téléchargements	12
Section V.4 Anti-plagiat	12
Section V.5 Respect des clauses contractuelles	12
Article VI. Traçabilité	13
Article VII. Confidentialité.....	13
Article VIII. Respect de la propriété intellectuelle	13
Article IX. Respect du cadre réglementaire Informatique et Libertés	14
Article X. Limitation des usages	14
Article XI. Entrée en vigueur de la charte.....	14



Préambule

La présente charte a pour objet de fixer les règles d'usage des moyens numériques de l'Université de Reims Champagne-Ardenne (URCA).

Par l'expression « moyens numériques », la présente charte vise tous les éléments ou toutes les ressources constituant le système d'information de l'URCA.

Ainsi, les moyens numériques représentent l'ensemble des logiciels et matériels, outils informatiques et services numériques, que l'URCA met à disposition de ses utilisateurs.

Les « **utilisatrices** » et « **utilisateurs** », au sens de la présente charte, sont définis comme l'ensemble des personnes ayant obtenu l'autorisation d'accéder au système d'information de l'URCA.

Ainsi sont notamment désignées :

- Toute agente ou tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'enseignement supérieur et de la recherche,
- Toute étudiante ou tout étudiant inscrit dans l'un des établissements de l'URCA,
- Tout prestataire ou partenaire ayant contracté avec l'URCA,
- Toute personne autorisée à accéder à un service numérique.

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

La présente charte a pour objet de fixer les règles d'usage des moyens numériques de l'URCA.

Ces règles ont pour but de contribuer à la sécurité du système d'information et de garantir l'intégrité et la confidentialité des données qui y sont hébergées.

L'usage raisonné des moyens numériques concourt par ailleurs à une conciliation saine et équilibrée des temps de vie professionnel et personnel.

Engagements de l'URCA

L'URCA porte à la connaissance de de l'utilisatrice ou de l'utilisateur la présente charte.

L'URCA met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisatrices et des utilisateurs.

L'URCA facilite l'accès des utilisatrices et des utilisateurs aux ressources du système d'information nécessaires. Les ressources mises à leur disposition sont prioritairement à usage universitaire mais l'établissement est tenu de respecter la vie privée de chacun dans les conditions décrites section II-1.

Engagements de l'utilisateur

L'utilisatrice ou l'utilisateur est responsable, en tout lieu, de l'usage qu'elle ou il fait du système d'information auquel elle ou il a accès. Elle ou il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels elle ou il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.

Les utilisatrices et les utilisateurs sont responsables de l'utilisation qu'ils font des ressources mises à leur disposition par l'URCA.



En tout état de cause, l'utilisatrice ou l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat. L'utilisatrice ou l'utilisateur dans son utilisation des outils numériques est soumis au droit français et communautaire.

Article I. Champ d'application

Les règles d'usage, de sécurité et de responsabilité figurant dans la présente charte s'appliquent à l'institution ainsi qu'à l'ensemble des utilisatrices et des utilisateurs internes et externes à l'URCA.

Les dispositions de la présente charte s'appliquent également aux utilisatrices et aux utilisateurs membres du personnel de l'URCA autorisés à exercer leurs missions dans les conditions de télétravail.

Les utilisatrices et les utilisateurs ayant des fonctions d'administratrice ou d'administrateur des moyens numériques ainsi que les éventuels sous-traitants seront soumis à une charte complémentaire et spécifique précisant leurs obligations particulières.

Article II. Conditions d'utilisation des systèmes d'information

Section II.1 Utilisation professionnelle / privée

L'URCA met à la disposition de ses utilisatrices et ses utilisateurs un ensemble d'outils et de services numériques à des fins professionnelles.

Au sens de la présente charte, l'usage des moyens numériques présente un caractère professionnel lorsqu'il intervient :

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

Les personnels s'engagent à utiliser les applications numériques fournies par l'Université. En cas de besoin, l'utilisatrice ou l'utilisateur demandera la validation d'un outil spécifique à sa hiérarchie ou au service informatique.

L'utilisation d'outils numériques à des fins privées de logiciels tiers doit être non lucrative et limitée, tant dans la fréquence que dans la durée. Elle ne doit nuire ni à la qualité du travail de l'utilisatrice ou l'utilisateur, ni au temps qu'il y consacre, ni au bon fonctionnement du service, et sous réserve du respect de la politique de sécurité et des obligations de loyauté et de confidentialité.

Toute information est réputée professionnelle 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 à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace prévu à cet effet et identifié sans ambiguïté comme tel. La sauvegarde régulière des données à caractère privé incombera à l'utilisatrice ou l'utilisateur.

Ainsi, tout utilisatrice ou tout utilisateur manifestera le caractère extra-professionnel d'une partie de ses données en adoptant, exclusivement, les termes « **privé** », « **personnel** » ou « **confidentiel** », pour nommer le dossier ou l'objet du message contenant ces informations.



Les utilisatrices et les utilisateurs se doivent d'adopter un comportement en lien avec leurs fonctions, vis-à-vis de l'établissement lors de l'utilisation des réseaux sociaux, des blogs et autres outils collaboratifs, qu'ils soient professionnels ou non professionnels.

Section II.2 Matériel personnel / professionnel

L'usage de ressources informatiques personnelles (un ordinateur, une tablette, un smartphone, un objet connecté, une clé USB, ...) achetées sur des crédits personnels, lorsqu'elles sont utilisées pour accéder au système d'information de l'URCA, ne doit pas remettre en cause ou affaiblir la sécurité en vigueur dans l'établissement.

Lorsque des données professionnelles (propriété de l'URCA) sont présentes sur des ressources informatiques personnelles, il incombe à l'utilisatrice ou à l'utilisateur de mettre tout en œuvre pour protéger ces données.

Le personnel disposant de ressource informatique et/ou audiovisuelle professionnelle (un ordinateur, une tablette, un smartphone, un objet connecté, une clé USB, connectique, vidéoprojecteur, ...) fourni par l'établissement, la composante, le laboratoire, ..., accepte la politique de gestion des ressources mise en place par l'URCA. A la fin de la mission lui ayant valu la mise à disposition du matériel, l'utilisatrice ou l'utilisateur s'engage à le restituer à l'établissement dans un état compatible avec un réemploi immédiat.

Section II.3 Outils de communication / Cloud computing

L'évolution des outils de communication sous différentes formes (réseaux sociaux, forums, espaces de contribution, messageries instantanées, ...) et utilisés dans un cadre personnel sont autorisés à la condition d'un usage raisonnable et raisonné. L'utilisation à des fins d'échanges de ces différents outils dans un cadre personnel et/ou professionnel doit toujours être cordiale.

Il est à rappeler auprès de toutes les utilisatrices et tous les utilisateurs de l'URCA leur responsabilité, ainsi que leurs obligations attendant à leur statut, même en cas de publications réalisées en dehors du temps de travail.

Dès lors que l'université met à disposition des moyens numériques, il convient de préciser que la responsabilité de l'URCA peut être engagée eu égard aux agissements de ses utilisatrices et de ses utilisateurs sur les outils de communication. L'URCA se réserve le droit d'ester en justice dans les cas les plus délictueux.

L'usage de service de « *Cloud computing* » (informatique dans les nuages) externes à l'URCA est toléré. Toutefois, il est absolument primordial que les données sensibles (données de recherche, données administratives, ...) du système d'information ne sortent pas du périmètre maîtrisé par l'URCA.

Section II.4 Continuité de service : gestion des absences et des départs

Afin d'assurer la continuité de service, l'utilisatrice ou l'utilisateur doit privilégier le dépôt de ses fichiers de travail et d'en assurer l'accessibilité, sur des zones partagées par les membres de son service ou de son équipe.

Concernant les données professionnelles : il appartient à la cheffe ou au chef de service de l'utilisatrice ou de l'utilisateur de s'assurer qu'elle ou il a accès aux données professionnelles nécessaires à la continuité de service et d'autoriser expressément, le cas échéant, toute copie totale ou partielle de ces données par l'utilisatrice ou l'utilisateur avant son départ. Cette autorisation est remise à l'utilisatrice ou à l'utilisateur.



Dans le cadre de l'harmonisation des durées d'accès au Système d'Information (SI), les durées suivantes sont mises en place :

- Concernant les étudiantes et les étudiants, l'accès informatique est valable tout au long de l'année universitaire sur laquelle ils sont inscrits administrativement, prolongé d'une durée de **2 mois**. L'accès sera automatiquement re prolongé sous réserve d'une nouvelle inscription administrative de l'étudiante ou de l'étudiant dans l'année universitaire suivante. Un délai de prolongation supérieur est autorisé pour certaines formations, en fonction du calendrier pédagogique voté annuellement par l'établissement. La durée maximum de cette prolongation est portée à 4 mois (31/12) après la fin d'année universitaire.
- Concernant les agentes et les agents, l'accès informatique est valable tout au long de la période d'activité de l'agente ou de l'agent jusqu'à sa date de fin d'activité prolongée d'une durée de **2 mois**. Certains accès informatiques seront fermés pour l'agente ou l'agent dès la fin de son activité en raison de mesures de sécurité informatique.

Il est de la responsabilité des étudiantes, des étudiants et des personnels de récupérer leurs données avant leur départ.

En tout état de cause les données non situées dans les répertoires « **privé** », « **personnel** » ou « **confidentiel** », sont considérées comme des données appartenant à l'établissement qui pourra en disposer, sans porter atteinte au droit de la propriété intellectuelle des enseignantes et des enseignants et des enseignantes-chercheuses et des enseignants-chercheurs sur leurs cours de production.

Section II.5 Droit à la déconnexion et l'usage de la messagerie à l'URCA

Le développement du numérique favorise de nouvelles formes de travail et brouille la limite entre vie personnelle et vie professionnelle. Dans ce contexte, il apparaît important de rappeler un certain nombre de recommandations qui doivent s'appliquer à l'ensemble des membres de la communauté universitaire :

- Tous les personnels, quels que soient leur grade, leur statut ou leur emploi sont invités à adopter une attitude raisonnée et éthique dans l'utilisation de la messagerie professionnelle, qui respecte les personnes et leur vie privée,
- L'usage de la messagerie doit être approprié et ne peut se substituer au dialogue ou aux échanges entre les personnes. Ce dialogue et ces échanges contribuent au lien social,
- L'usage de la messagerie doit se faire dans le respect des règles de courtoisie et de politesse,
- L'envoi de messages électroniques est à éviter (sauf urgence) en dehors des horaires habituels de travail, soit entre 19h et 8h, le week-end et les jours fériés,
- Les personnels ne sont pas tenus de répondre aux messages électroniques en dehors des horaires habituels de travail, pour préserver au mieux la distinction entre vie privée et vie professionnelle.

Article III. Principes de sécurité

Section III.1 Règles de sécurité applicables

L'URCA met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisatrices et des utilisateurs.

L'utilisatrice ou l'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisatrice ou à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des systèmes d'information mis à sa disposition lui impose :



- De garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers, en particulier de ne pas les afficher à la vue de tous,
- De respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'une autre utilisatrice ou d'un autre utilisateur, ni chercher à les connaître,
- De respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisatrice ou de l'utilisateur nécessite plusieurs précautions, de la part de l'URCA via sa Direction du Numérique :

- Veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de continuité du service mises en place par la hiérarchie (Cf. section II.2),
- Limiter l'accès aux seules ressources pour lesquelles l'utilisatrice ou l'utilisateur est expressément habilité ;

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

- De verrouiller son poste de travail en cas d'absence et d'utiliser les économiseurs d'écran avec mot de passe afin de préserver l'accès à son poste de travail,
- S'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles elle ou il n'a pas reçu d'habilitation explicite,
- Ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'institution,
- Ne pas installer, télécharger ou utiliser sur le matériel de l'URCA, des logiciels ou progiciels sans respecter les droits de licence ; les logiciels doivent être utilisés dans les conditions des licences souscrites,
- Se conformer aux dispositifs mis en place par l'établissement pour lutter contre les virus et les attaques par programmes informatiques,
- 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.

Devoirs de signalement et d'information

L'utilisatrice ou l'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, suspicion d'une usurpation d'un code d'accès. Elle ou il signale également à sa ou son responsable toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation. L'utilisatrice ou l'utilisateur ou sa hiérarchie informera obligatoirement les RSSI (Responsables de la Sécurité des Systèmes d'Information) de l'établissement concerné à l'adresse de contact rssi@univ-reims.fr

Section III.2 Mesures de contrôle de la sécurité

L'utilisatrice ou l'utilisateur est informé :

- Que pour effectuer la maintenance corrective, curative ou évolutive, l'URCA se réserve la possibilité de réaliser des interventions (le plus souvent à distance) sur les ressources matérielles et logicielles mises à sa disposition,
- Qu'une maintenance à distance est précédée d'une information de l'utilisatrice ou l'utilisateur,
- Que toute situation bloquante pour le système ou générant une difficulté technique, pourra conduire à l'isolement du poste voire à la suppression des éléments en cause,
- Que les outils du système d'information dont la conformité au Règlement Général sur la Protection des Données (RGPD) et l'information aux personnes concernées ont été effectuées peuvent donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire, de suivi



fonctionnel, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable,

- Qu'il lui est formellement interdit de désinstaller ou de contourner les outils d'administration mis en place par l'informatique de proximité de l'URCA,
- Que si l'ordinateur doit être réinstallé, l'utilisatrice ou l'utilisateur doit faire appel à l'informatique de proximité pour l'accompagner dans cette démarche,
- Qu'il lui est interdit de modifier et/ou supprimer le compte administrateur sur l'ordinateur qu'elle ou il a reçu de la part de l'URCA,

Tout ordinateur commandé sur les crédits de l'URCA doit être intégré dans son système d'authentification. Les personnels chargés du bon fonctionnement des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

Section III.3 Protection antivirale

L'URCA a déployé une protection logicielle généralisée non seulement sur les serveurs mais aussi les postes de travail des utilisateurs.

Le but d'un anti-virus est de protéger toutes les machines du parc contre les attaques provoquées par des codes malveillants. Sur chaque poste utilisateur est installé un client anti-virus. Il est interdit par la présente charte de désactiver, d'altérer le fonctionnement ou de désinstaller ce client. Il est aussi interdit d'utiliser d'autres logiciels (anti-virus ou autres) susceptibles d'entraîner un dysfonctionnement de l'anti-virus installé en exécution de la stratégie de sécurité de l'URCA. L'URCA ayant souscrit dans le cadre d'un marché national pour la fourniture d'antivirus, il est formellement interdit d'utiliser un autre antivirus ne relevant pas de ce marché sur un poste de l'université.

Article IV. Numérique Responsable

Section IV.1 Sobriété énergétique

- Extinction des appareils : Eteindre les appareils (ordinateurs, écrans, imprimantes) lorsqu'ils ne sont pas utilisés, surtout la nuit et le week-end sauf exception spécialement affiché sur les équipements.
- Mode veille : Utiliser les modes de veille et d'économie d'énergie sur les appareils.
- Chargement responsable : Débrancher les chargeurs lorsque les appareils sont entièrement chargés pour éviter la consommation d'énergie inutile.

Section IV.2 Utilisation rationnelle des ressources

- Impression raisonnée : Imprimer uniquement lorsque nécessaire et privilégier les fonctions recto-verso et le recyclage de papier brouillon pour économiser le papier.
- Dématérialisation : Privilégier les documents numériques et les échanges électroniques pour réduire l'utilisation de papier.
- Tri des fichiers : Faire régulièrement le tri des fichiers numériques pour supprimer ceux qui ne sont plus nécessaires et limiter le stockage inutile (un même fichier sauvegardé sur un espace de stockage externe est dupliqué sur différents espaces, multipliant ainsi le volume numérique utilisé)
- Archivage : Effectuer un tri régulier ou une suppression régulière des fichiers, des mails et des pièces jointes préalablement sauvegardées.
- Visionnage : Dans la mesure du possible télécharger les films ou les vidéos pour limiter le visionnage en streaming et supprimer ces fichiers lorsqu'ils deviennent inutiles.



- Intelligence artificielle : L'utilisation exponentielle de l'I.A. génère des coûts environnementaux non négligeables. La consommation de ressources en puissance de calcul n'est pas toujours efficiente et il est important de maîtriser la façon de l'utiliser en cherchant à minimiser l'impact environnemental.

Section IV.3 Économie circulaire

- Achat responsable : Toute demande d'achat de matériel numérique doit impérativement transiter par la Direction du Numérique. En respectant les spécifications demandées par l'utilisatrice ou l'utilisateur, la Direction du Numérique privilégie ceux qui sont économes en énergie (norme Energy Star) et issus de sources responsables (Ecolabel). Il est important de ne commander que les seuls équipements nécessaires.
- Réparation et réutilisation : Faire réparer les appareils en cas de panne et envisager la réutilisation d'équipements d'occasion ou reconditionné.
- Recyclage : Le recyclage des déchets électroniques est organisé par la Direction du Numérique qui sera sollicitée préalablement avant toute démarche de gestion de la fin de vie des équipements électroniques.
- Cycle de vie : Un renouvellement d'appareil ne peut pas se faire avant une certaine durée prescrite par les recommandations du schéma directeur Développement Durable et Responsabilité Sociale des Entreprises (DD&RSE), sauf défaillance manifeste du matériel.

Section IV.4 Communication numérique éco-responsable

- Choix des outils : Utiliser les outils de communication numériques (visioconférence, messagerie instantanée) pour réduire les déplacements et leur empreinte carbone. Mais surtout utiliser les outils les plus adaptés selon le contexte et le but de votre réunion.
- Messagerie : Limiter le nombre de destinataires dans les correspondances. Éviter les « réponses à tous » quand cela ne s'avère pas nécessaire. Utiliser des liens vers des fichiers plutôt que joindre un fichier aux mails.

Article V. Communication électronique

Section V.1 Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de l'URCA.

La messagerie est un outil de travail destiné à des usages professionnels : elle peut constituer le support d'une communication privée telle que définie à la section II.1.

(a) Adresses électroniques

L'URCA s'engage à mettre à la disposition de l'utilisatrice ou de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

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.

Des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d' « utilisatrices et d'utilisateurs », pourront être mises en place par l'URCA.

Certaines listes institutionnelles sont utilisées au sein de l'établissement et ne peuvent donner lieu à un désabonnement de la part de l'utilisatrice ou de l'utilisateur.



(b) Contenu des messages électroniques

Par référence à l'article II, section II.1, tout message sera réputé professionnel sauf s'il comporte en objet la mention « **privé** », « **personnel** » ou « **confidentiel** », ou s'il est stocké dans un espace spécifique de données identifié comme tel.

Pour préserver le bon fonctionnement des services, des limitations pourront être mises en place. En particulier des solutions de traitement des messages indésirables (spam, contrôle des virus, ...) seront déployées.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature.

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.

(c) 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. Elle ou il doit veiller à ce que la diffusion réfléchie des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service. Des recommandations sont présentées dans le guide pratique de l'utilisateur annexé à la présente charte.

(d) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent juridiquement former un contrat, sous réserve du respect des conditions fixées par les articles 1101 et suivants du Code civil.

L'utilisatrice ou l'utilisateur doit, en conséquence, être vigilant sur le contenu des messages électroniques quelle ou 'il échange à l'instar des courriers traditionnels.

En application du Code des relations entre le public et l'administration (article L112-8 et suivants), désormais les échanges électroniques entre l'administration et une ou un usager ou une ou un de ses agentes ou agents peuvent valoir décision administrative.

Les échanges électroniques de ce type doivent par conséquent se conformer aux exigences légales en vigueur pour ce genre d'actes administratifs.

Un courriel peut engager administrativement l'établissement.

(e) Stockage et archivage des messages

Chaque utilisatrice ou 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.

Le guide pratique de l'utilisateur, annexé à la présente charte, présente un ensemble de règles impératives et de recommandations dont le respect garantit la conservation de ces données.

(f) Gestion des absences

En cas d'absence de l'utilisatrice ou de l'utilisateur, celle-ci ou celui-ci s'engage à utiliser le gestionnaire d'absence de l'outil de messagerie qui permet de renseigner le texte de la réponse automatiquement



adressée à chaque expéditrice ou expéditeur en précisant en particulier la période d'absence et les autres adresses où le message peut être envoyé en cas de nécessité.

Lors de la mutation d'une « utilisatrice » ou d'un « utilisateur », il convient d'éviter que sa boîte de messagerie continue à recevoir des messages au titre des fonctions qu'elle ou il quitte.

En cas de départ définitif de l'institution pour éviter que des courriers électroniques ne soient pas relevés, que des boîtes de messagerie demeurent inutilisées, que des messages personnels ou confidentiels soient lus par des agentes ou des agents qui ne sont pas destinataires, l'utilisatrice ou l'utilisateur s'engage à suivre la procédure suivante :

- L'utilisatrice ou l'utilisateur envoie un message à ses correspondants habituels leur indiquant la date de son départ définitif et leur signalant la boîte de messagerie à laquelle ils devront envoyer leurs messages à partir de cette date au titre des fonctions qu'elle ou il quitte (adresse de messagerie de sa ou son successeur s'il est connu, boîte de l'intérimaire ou boîte fonctionnelle),
- Juste avant son départ, l'utilisatrice ou l'utilisateur archive dans un fichier les messages qu'elle ou il doit transmettre à son successeur et remet ce fichier à sa supérieure ou son supérieur hiérarchique,
- L'utilisatrice ou l'utilisateur s'engage à ré-aiguiller les messages qu'elle ou il reçoit durant la période où la messagerie reste active après son départ et qui sont destinés à son ancien service.

En cas de décès de l'utilisatrice ou de l'utilisateur ou si elle ou il s'absente sans préavis et est injoignable, l'institution se réserve le droit de supprimer tout message de réponse automatique ou de redirection qui impacterait le bon fonctionnement des services. Un autre message de réponse automatique pourra être rajouté en tant que de besoin à la discrétion de l'institution. Le service en charge de la messagerie, sur demande écrite de la présidente ou du président et selon les modalités définies à l'article (g), pourra accéder à la boîte de messagerie afin de transmettre les messages nécessaires à la continuité de service. C'est pourquoi il est recommandé d'utiliser les adresses de messagerie fonctionnelles plutôt que nominatives.

(g) Décès ou départ soudain de l'utilisateur

Dans le cas du décès ou d'un départ de l'utilisatrice ou de l'utilisateur et notamment pour les besoins de la continuité de service, l'institution pourra être amenée à supprimer tout message de réponse automatique qui aurait été rédigé et à mettre en place un nouveau message indiquant vers qui les expéditeurs doivent se tourner. Si une redirection des messages électroniques était en place, cette dernière pourra également être supprimée. De plus, le compte de messagerie est verrouillé ainsi que les accès aux services numériques à partir du compte de cette personne, 24 heures maximum après la saisie de l'information du décès ou du départ dans la base de données des ressources humaines ou de la scolarité par les services habilités. Les données de l'utilisateur sont cependant conservées afin de pouvoir être fournies en cas de réquisition judiciaire ou sur demande de la Présidente ou du Président de l'institution pour assurer la continuité de service.

En cas de décès, la famille ne peut demander sans décision de justice la récupération des données.

(h) Modalités d'accès à une boîte de messagerie

Sur demande de la Présidente ou du Président de l'institution et en cas d'absence prolongée ou de décès d'un personnel, en invoquant la continuité de service pour justifier la transmission de certains messages, dans ce cas, l'accès à la messagerie est strictement encadré avec la présence de témoins (la ou le Responsable de la sécurité des systèmes d'information et la Déléguée ou le Délégué à la protection des données (RSSI et DPO)) qui garantissent la procédure. Les messages dont le sujet comporte « **privé** », « **confidentiel** » ou « **personnel** » ou dont l'objet est sans rapport avec la demande de continuité de service ne peuvent être accédés.



Section V.2 Internet

Il est rappelé que le réseau Internet est soumis à l'ensemble des règles de droit en vigueur.

L'utilisation de la technologie Internet (et par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'URCA.

L'URCA met à la disposition de l'utilisatrice ou de l'utilisateur un accès Internet chaque fois que cela est possible.

Internet est un outil de travail destiné à des usages professionnels : il peut constituer le support d'une communication privée telle que définie en section II.1, dans le respect de la réglementation en vigueur.

Il est rappelé que la consultation volontaire de contenus à caractère illicite (notamment pédopornographique, raciste, xénophobe, incitation à la violence, ...) est proscrite.

Les utilisatrices et les utilisateurs sont informés qu'en considération de la mission éducative de l'établissement, la consultation volontaire et répétée de contenus à caractère pornographique depuis les locaux de l'URCA est proscrite, sauf en cas de travaux de recherches scientifiques sur ce sujet.

Section V.3 Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, doit s'effectuer dans le respect des droits de propriété intellectuelle tels que définis à l'article VIII.

L'URCA 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'information, tels les virus, code malveillant ou programmes espions.

12

Section V.4 Anti-plagiat

La mise à disposition d'un outil de détection de similitude ou anti-plagiat, s'inscrit dans une perspective non répressive et d'aide à la prise de décision.

Par conséquent, cet outil et les indicateurs fournis, ne peuvent fonder à eux seuls une décision de sanction.

L'accès à l'outil est activé par le Service des Usages du Numérique, après une prise de contact avec l'un des référents anti-plagiat ou la participation à une formation spécifique.

Cet outil ne concerne que les travaux des étudiantes et des étudiants ou stagiaires et uniquement dans le contexte de l'enseignement.

Section V.5 Respect des clauses contractuelles

L'usage des ressources documentaires électroniques éditoriales doit respecter les conditions contractuelles des licences souscrites par l'université.

D'une façon générale, et sauf mention contraire explicite dans la licence, indiquée clairement sur le site de la bibliothèque, les éditrices et les éditeurs n'autorisent qu'une utilisation « raisonnable » et personnelle des ressources documentaires électroniques, dans un but strictement non-commercial et à des fins pédagogiques ou de recherche.



Les termes ci-dessus doivent être entendus de la manière suivante :

- Utilisation raisonnable : L'utilisatrice ou l'utilisateur s'engage à ne pas télécharger de livres complets (hors livres numériques proposés en tant qu'entités téléchargeables sur des plateformes dédiées, ou sur des liseuses ou tablettes de lecture prêtées par la bibliothèque) ou de fascicules entiers de revues, ainsi qu'à ne pas utiliser d'aspirateur de site web.
- Utilisation personnelle : L'utilisatrice ou l'utilisateur s'engage à faire un usage personnel des ressources électroniques documentaires : aucune diffusion à une personne extérieure à l'université, même à titre gratuit, n'est autorisée, ni sous forme de copies imprimées, ni sous forme électronique.
- Utilisation dans un cadre pédagogique ou de recherche : L'utilisatrice ou l'utilisateur s'engage à n'utiliser les ressources documentaires électroniques que dans le cadre strict de ses études, de son enseignement ou de sa recherche.

Aucune utilisation à des fins commerciales n'est autorisée. Les documents ou les données ainsi que leur exploitation ne peuvent pas être destinés à une entreprise dans laquelle une étudiante ou un étudiant serait en stage, ou être utilisés par un enseignant ou un étudiant dans le cadre d'une activité professionnelle pour le compte d'un cabinet ou d'une entreprise.

Article VI. Traçabilité

Cette traçabilité est mise en place conformément au Règlement Général sur la Protection des Données (RGPD) et à la loi du 6 janvier 1978 modifiée.

Les utilisatrices et 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.

Article VII. Confidentialité

Chaque « utilisatrice » ou « utilisateur » a une obligation de confidentialité et de discrétion à l'égard des informations et documents électroniques à caractère confidentiel auxquels elle ou il a accès dans le système d'information. Le respect de cette confidentialité implique notamment :

- De veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations,
- De respecter les règles d'éthique professionnelle et de déontologie, ainsi que l'obligation de réserve et le devoir de discrétion.

Article VIII. Respect de la propriété intellectuelle

L'URCA rappelle que l'utilisation des moyens numériques 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 ou utilisateur doit :

- Utiliser les logiciels dans le strict respect des licences souscrites,
- S'abstenir de 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 autre droit privatif, sans avoir obtenu préalablement l'autorisation du ou des titulaires de ces droits.



Article IX. Respect du cadre réglementaire Informatique et Libertés

L'utilisatrice ou l'utilisateur est informé de la nécessité de respecter le Règlement Général sur la Protection des Données (règlement UE 2016/676 dit RGPD) et la loi du 6 janvier 1978 modifiée (loi Informatique et Libertés).

Les données à caractère personnel sont des informations qui permettent l'identification des personnes physiques auxquelles elles se rapportent, directement ou indirectement, et à partir d'une seule donnée ou à partir du croisement d'un ensemble de données.

Toutes les créations ou modifications de fichiers comprenant ce type d'informations 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 réglementation en vigueur.

En conséquence, toute utilisatrice ou tout utilisateur souhaitant procéder à une telle création ou modification de fichiers devra préalablement contacter le DPO (Délégué à la Protection des Données) de l'URCA à l'adresse suivante : dpo@univ-reims.fr

L'utilisatrice ou l'utilisateur a l'obligation d'alerter le DPO et le RSSI en cas de violation de données à caractère personnel.

De plus, conformément aux dispositions du Règlement Général sur la Protection des Données (RGPD) et à la loi du 6 janvier 1978 modifiée, chaque utilisatrice ou chaque utilisateur dispose d'un droit d'accès, de rectification et d'effacement ainsi que d'un droit d'opposition, d'un droit à la limitation du traitement et d'un droit à la portabilité relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information.

Article X. Limitation des usages

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisatrice ou l'utilisateur à des fins extraprofessionnelles, est passible de sanctions disciplinaires et pénales.

Article XI. Entrée en vigueur de la charte

La présente charte sera intégrée au règlement intérieur de l'URCA.

La présente charte s'ajoute à tous les autres documents ou chartes.

Sont annexés à cette charte les documents suivants :

- guide d'utilisation,
- annexe juridique.

Approuvée par le conseil d'administration du 01/07/2025

