



# RÉGION ACADÉMIQUE BRETAGNE

*Liberté  
Égalité  
Fraternité*

**Charte d'usage du système d'information  
de la Région académique de Bretagne  
pour les personnels**

PRÉAMBULE.....	3
1. Engagement de l’institution .....	3
2. Engagement de l'utilisateur.....	3
ARTICLE 1 – CHAMP D’APPLICATION.....	4
ARTICLE 2 – CONDITIONS D’APPLICATION DU SYSTÈME D’INFORMATION.....	4
1. Utilisation professionnelle / privée .....	4
2. Continuité de service : gestion des absences et départs.....	4
3. Accès aux données.....	5
4. Offre de service .....	5
ARTICLE 3 – Mise à disposition D’UN COMPTE académique UTILISATEUR.....	5
1. Délivrance du compte.....	6
2. Initialisation du mot de passe.....	6
3. Durée de vie du compte .....	6
ARTICLE 4 – Mise à disposition de MATÉRIEL INFORMATIQUE.....	6
1. Engagement des personnels.....	6
2. Engagement de l’institution .....	7
3. Durée du prêt et restitution.....	8
ARTICLE 5 – PRINCIPES DE SÉCURITÉ.....	8
1. Règles de sécurité applicables.....	8
2. Mesures de sécurité .....	9
ARTICLE 6 – COMMUNICATION ELECTRONIQUE.....	10
1. Messagerie électronique .....	10
2. Internet .....	12
ARTICLE 7 – TRACABILITÉ .....	13
ARTICLE 8 – PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL.....	13
ARTICLE 9 – RÈGLEMENT DES LITIGES .....	14
ARTICLE 10 – ENTRÉE EN VIGUEUR DE LA CHARTE.....	14
ARTICLE 11 – DISPOSITIONS FINALES.....	15

Par « institution », il faut entendre tout service de la Région académique de Bretagne y compris les services déconcentrés (rectorat, DSDEN, circonscriptions du 1er degré), les écoles du premier degré, les établissements d'enseignement du second degré et les Centres d'Information et d'Orientation.

Le Système d'Information (SI) recouvre l'ensemble des ressources matérielles et logicielles, les applications, les bases de données et les réseaux de télécommunications pouvant être mis à disposition pour le fonctionnement de l'institution.

Les équipements numériques (ordinateurs portables, tablettes, téléphones portables, etc) sont constitutifs du système d'information dès lors qu'ils sont mis à disposition par l'institution ou qu'ils sont connectés au réseau de l'institution quand ils sont personnels.

Le terme « utilisateur » recouvre tout personnel ayant accès, dans le cadre de l'exercice de son activité professionnelle, au système d'information quel que soit son statut. Il s'agit notamment de :

- tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'Éducation nationale,
- les partenaires institutionnels (opérateurs, collectivités territoriales, établissements d'enseignement relevant d'autres ministères)
- tout prestataire ayant contracté avec l'institution ou avec une collectivité territoriale ayant compétence partagée avec l'État en matière d'éducation.

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

La présente charte définit les règles d'usages et de sécurité que l'institution et l'utilisateur doivent respecter : elle précise les droits et devoirs de chacun.

### 1. Engagement de l'institution

L'institution porte à la connaissance de l'utilisateur la présente charte.

Elle met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs et de leurs données.

L'institution facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont à usage professionnel mais l'institution est tenue de respecter la vie privée de chacun.

Dès qu'ils sont en fin de fonction, les utilisateurs perdent leurs droits d'accès aux applications du système d'information.

Concernant les agents des partenaires institutionnels, leur fin de fonction est communiquée sans délai à la Région académique par l'organisme de rattachement.

### 2. Engagement de l'utilisateur

L'utilisateur est responsable, en toutes circonstances, 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 des documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie, des lois et règlements en vigueur.

En cas de non-respect, la responsabilité de l'utilisateur pourra être engagée. Tout abus de l'utilisation des ressources mises à disposition à des fins extra-professionnelles peut être de nature à enclencher une procédure disciplinaire à son encontre. Par ailleurs, le responsable hiérarchique pourra, sans préjuger des poursuites ou procédures pouvant être engagées, limiter les usages par mesure conservatoire.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut.

## ARTICLE 1 – CHAMP D'APPLICATION

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

L'usage des systèmes d'information à caractère syndical est encadré par les directives ministérielles relatives à l'usage des Technologies de l'Information et de la Communication (TIC) par les Organisations Syndicales (OSTIC).

## ARTICLE 2 – CONDITIONS D'APPLICATION DU SYSTÈME D'INFORMATION

### 1. Utilisation professionnelle / privée

Le système d'information est un outil de travail réservé à un usage professionnel (administratif et pédagogique), mais peut être utilisé à titre privé de manière exceptionnelle. Cette utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée, et ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée qui doivent être qualifiées de « personnel » ou « privé ». En effet, en l'absence de ce qualificatif, l'information contenue dans l'outil informatique mis à la disposition de l'agent pour l'exécution de son travail est présumée avoir un caractère professionnel, auquel le recteur ou son représentant pourra avoir accès en cas de besoin.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource. La sauvegarde régulière des données à caractère privé incombe à l'utilisateur. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace.

### 2. Continuité de service : gestion des absences et départs

L'utilisateur est incité à informer sa hiérarchie des modalités permettant l'accès éventuel aux ressources mises spécifiquement à sa disposition aux seules fins d'assurer la continuité du service<sup>1</sup>.

Aussi, les personnels, notamment ceux exerçant une responsabilité administrative, devront, en cas d'impossibilité prolongée d'accès à leur messagerie, faire en sorte qu'en collaboration avec leur responsable hiérarchique les messages nécessaires au bon fonctionnement du service qui leur parviendraient dans leur boîte nominative ne soient pas perdus. Ils devront notamment utiliser la fonction de notification d'absence de la messagerie pour indiquer à leurs interlocuteurs leur absence et la boîte vers laquelle leurs messages devront être, si besoin, réémis.

Le recteur peut imposer la mise en place de ce message d'absence dans le but exclusif de l'intérêt et de la continuité du service.

### 3. Accès aux données

La gestion de données confidentielles relatives à des personnes est réservée aux personnels dûment habilités.

Les personnels tels que les médecins scolaires, médecins de prévention, infirmier(ère)s ou assistant(e)s sociaux(les) sont amenés, dans le cadre de leurs fonctions, à gérer des données sensibles sur d'autres personnes. En cas d'absence ou de départ, l'accès à ces données ne pourra se faire que par une personne ayant la même qualité et dans le strict respect du secret médical ou professionnel.

### 4. Offre de service

L'institution propose à l'utilisateur un ensemble de services lui permettant de travailler dans un environnement professionnel et sécurisé.

Portée à la connaissance de l'utilisateur, cette offre de services peut comprendre selon sa fonction :

- la mise à disposition d'un poste de travail, individuel ou partagé, fixe ou mobile ;
- la mise à disposition d'un espace de stockage de ses données ;
- la mise à disposition d'un accès à l'espace de partage de son service ou de son établissement ;
- la mise à disposition d'un service de stockage personnel, d'un gestionnaire de mots de passe, de services de communication et de collaboration au sein de l'espace numérique de travail Toutatice ;
- un service de téléphonie ;
- un service d'impression.

Dans le cadre d'une situation de télétravail, l'utilisateur accède à l'offre de service exclusivement par le biais de son poste de travail professionnel et d'un réseau privé virtuel, soumis à une authentification forte (clé OTP logicielle ou matérielle). Les modalités de télétravail sont précisées dans le protocole signé par le télétravailleur et son responsable hiérarchique.

## ARTICLE 3 – MISE A DISPOSITION D'UN COMPTE ACADEMIQUE UTILISATEUR

---

<sup>1</sup> À l'exclusion de la communication du mot de passe, qui doit rester personnel en toute circonstance.

Un compte utilisateur nominatif est délivré sous la forme d'un identifiant et d'un mot de passe à chaque agent régulièrement inscrit dans les bases des ressources humaines de la Région académique pour pouvoir assurer ses missions. Le compte académique permet à l'agent de se connecter à son poste de travail, sa messagerie, ses applications métiers, les espaces collaboratifs et l'ENT Toutatice.

## 1. Délivrance du compte

Une fois l'agent saisi dans les systèmes d'information des ressources humaines par les services de gestion concernés, la création du compte utilisateur prend 48h.

Une fois le compte créé, le supérieur hiérarchique ou le secrétariat de la division doit saisir les informations d'habilitation afin que l'agent puisse disposer des droits adéquats dans les systèmes d'informations dont il aura l'usage.

Ces saisies doivent donc être anticipées pour permettre aux agents de pouvoir assurer leurs missions dès leur prise de fonction.

## 2. Initialisation du mot de passe

Le jour de la prise de fonction l'agent doit initialiser son mot de passe sur Toutatice avant de pouvoir utiliser son compte.

Pour se faire l'agent reçoit une notification dans son établissement ou service d'affectation. Il doit utiliser la procédure de recouvrement de mot de passe qui y est indiquée muni de son NUMEN et de son identifiant.

A la suite de la procédure d'initialisation du mot de passe le compte est opérationnel.

## 3. Durée de vie du compte

Les habilitations aux services numériques (hors messagerie) liées au compte sont supprimées automatiquement le jour de la fin de fonction de l'agent.

La boîte aux lettres nominative professionnelle est maintenue pendant une durée de 12 mois. Le compte de messagerie est quant à lui supprimé au mois d'août de l'année qui suit la date de départ de l'agent de la Région académique. Les agents en détachement à l'extérieur de la Région académique conservent leur compte utilisateur pendant toute la durée du détachement.

# ARTICLE 4 – MISE A DISPOSITION DE MATÉRIEL INFORMATIQUE

La présente charte définit également les conditions d'utilisation et les modalités de prêt des matériels informatiques sur site, dans le cadre du télétravail, de travail à distance ou de mobilité validées par le chef de service, acquis par l'État, mis à disposition par l'institution aux personnels selon leur fonction ou mission.

## 1. Engagement des personnels

### 4.1.1. Protection de l'équipement

L'utilisateur s'engage à apporter tout le soin nécessaire aux matériels prêtés, à sa garde et à sa conservation. Tout dysfonctionnement ou dommage du matériel devra être notifié par le bénéficiaire via le dispositif d'assistance académique au plus vite.

En cas de vol de l'équipement, il appartiendra à l'utilisateur d'alerter la direction régionale des systèmes d'information « DRASI », dans un délai de 72h maximum à l'adresse : [ce.drasi@ac-rennes.fr](mailto:ce.drasi@ac-rennes.fr).

Pendant les périodes de vacances, l'utilisateur s'engage à laisser son équipement informatique sur site, sauf nécessité de services convenue avec son responsable hiérarchique.

Afin d'assurer la protection de l'équipement et des données, des mesures de sécurité ont été mises en œuvre : antivirus, chiffrement du disque dur, certification des logiciels installés. Par conséquent, même s'il dispose d'un profil administrateur du poste de travail mis à disposition, l'utilisateur s'engage à ne pas changer la configuration de l'équipement sans accord préalable écrit de la DSII. Une demande d'assistance auprès de la DSII devra être effectuée pour obtenir cet accord.

#### **4.1.2. Sauvegarde des données**

Pour les postes intégrés au domaine académique et pour assurer la sauvegarde des fichiers, l'agent s'engage à enregistrer ses fichiers dans le répertoire « Mes documents » qui est synchronisé avec les serveurs de stockage académiques et sauvegardé. Dans le cas du télétravail, cette synchronisation se réalise à condition d'établir la connexion au réseau virtuel privé (VPN.).

Pour les agents en situation de travail nomade, il est recommandé d'utiliser la solution de stockage en ligne de la Région académique pour assurer la sauvegarde continue de leurs fichiers.

## **2. Engagement de l'institution**

#### **4.2.1. Conditions d'installation et de livraison du matériel**

Toute demande de mise à disposition d'un équipement informatique doit être réalisée par le responsable de l'agent ou son secrétariat via le dispositif d'assistance de la DSII (<https://assistance.ac-rennes.fr>). Pour la mise à disposition d'un ordinateur, un temps de préparation de 7 jours est nécessaire à la DSII à partir de la réception de la demande. Les logiciels standards nécessaires aux travaux de l'agent sont installés en rapport avec son usage professionnel. Pour que cet ordinateur soit pleinement opérationnel, il est nécessaire que l'agent soit présent dans les bases de données des ressources humaines.

Suite à la notification de réception et de préparation du poste informatique qui sera transmise par mail à l'agent, le matériel devra être directement enlevé par l'agent sur rendez-vous pris via le dispositif d'assistance de la DSII (<https://assistance.ac-rennes.fr>).

En cas de remplacement ou de renouvellement d'un matériel, la DSII pourra procéder à la sauvegarde et la restauration des données professionnelles l'agent et récupérera l'ancien matériel.

Chaque équipement numérique mis à disposition d'un personnel en service déconcentré est référencé dans l'outil d'inventaire académique.

#### **4.2.2. Conditions matérielles et financières d'entretien et de réparation**

En cas de panne, d'obsolescence, de perte ou de vol, l'institution prendra en charge le remplacement du matériel. Le matériel dysfonctionnel devra être restitué à la DSII.

Pour tout cas de dysfonctionnement, l'agent prend contact avec le dispositif d'assistance de la DSII (<https://assistance.ac-rennes.fr>) pour traitement des suites à donner.

L'utilisateur s'engage à accepter de mettre le matériel à la disposition de la DSII durant les périodes nécessaires à son entretien et à sa maintenance.

L'utilisateur s'engage à ne pas procéder lui-même à des réparations. Il doit faire appel à la DSII en cas de dysfonctionnement de son équipement. La DSII procédera aux travaux de réparation et, en cas de besoin, proposera un matériel de substitution dans la mesure des stocks disponibles.

### 3. Durée du prêt et restitution

Le prêt de matériel est effectué pour une année scolaire, et tacitement reconduit.

Dans les trois cas suivants, le matériel devra être obligatoirement restitué à l'institution par l'utilisateur en prenant rendez-vous via le dispositif d'assistance de la DSII (<https://assistance.ac-rennes.fr>).

- Changement de fonction ne nécessitant plus ce type de matériel
- Changement de région académique/ d'établissement
- Fin de fonction / Départ à la retraite

Le matériel devra être restitué complet et en bon état de fonctionnement, une vérification de l'ensemble des composantes sera effectuée par la DSII lors de la remise du matériel.

Ce prêt pourra également être stoppé unilatéralement par lettre recommandée avec accusé de réception à tout moment notamment :

- En cas de détérioration volontaire des matériels ;
- En cas d'utilisation non conforme aux obligations contractées par les parties comme défini dans cette charte d'usage des systèmes d'information.

## ARTICLE 5 – PRINCIPES DE SÉCURITÉ

### 1. Règles de sécurité applicables

L'institution met en œuvre les mécanismes de protection appropriés sur le système d'information.

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 ressources matérielles et logicielles protégées d'un caractère privé.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est confiée.

La sécurité des systèmes d'information mis à sa disposition lui impose de :

- respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ;
- garder strictement confidentiel(s) son (ou ses) code(s) d'accès et ne pas le(s) dévoiler à un tiers y compris son supérieur hiérarchique ;
- ne pas conserver le mot de passe fourni initialement par l'institution en le modifiant dès le premier usage ;
- respecter la gestion des accès, et en particulier, ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs obligations :

#### 5.1.1. de la part de l'institution

- porter à la connaissance de l'utilisateur de manière explicite ses habilitations ;
- contrôler et mettre à jour les habilitations ;
- veiller à ce que les ressources sensibles ou confidentielles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie ;
- porter à la connaissance de l'utilisateur les éléments susceptibles de lui permettre de sécuriser l'usage du système d'information, dont le matériel personnel à usage professionnel.

### 5.1.2. de la part de l'utilisateur

- ne pas tenter d'accéder à des ressources du système d'information pour lesquelles il n'a pas reçu d'habilitation ;
- ne pas connecter 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'institution, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance sans autorisation de sa hiérarchie ;
- se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques ;
- avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute(s) violations, tentative de violation ou violation suspectée de la confidentialité des données à caractère personnel ainsi que tout incident de sécurité présentant un risque pour les droits et libertés des personnes auprès du délégué à la protection des données et du Responsable de la sécurité des systèmes d'information via : [alerte.ssi@ac-rennes.fr](mailto:alerte.ssi@ac-rennes.fr)
- signaler également à la personne responsable du site toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation ;
- ne pas enregistrer de données de l'institution en dehors du système d'information.

L'institution rappelle que l'utilisation des ressources informatiques et numériques implique le respect des droits de propriété intellectuelle. Ce principe s'applique également aux partenaires liés par convention ou contrat et plus généralement, à tous tiers titulaires de tels droits.

En conséquence, chaque 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 ;
- favoriser l'utilisation de ressources sous licences libres, en n'omettant pas de préciser sous quelles conditions cette ressource est partagée.

## 2. Mesures de sécurité

L'utilisateur est informé que :

- pour effectuer la maintenance corrective, curative ou évolutive, l'institution se réserve la possibilité de réaliser des interventions, le cas échéant à distance, sur les ressources mises à sa disposition ;

- une maintenance à distance est toujours précédée d'une information de l'utilisateur ;
- toute information présentant un risque pour le système d'information sera isolée et le cas échéant, elle sera supprimée ;
- le système d'information donne lieu à une surveillance du bon fonctionnement et à un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels chargés des opérations de contrôle du système d'information sont soumis à des règles de confidentialité renforcée décrits dans la charte des administrateurs. Ils ne peuvent pas divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions : ces informations sont couvertes par le secret des correspondances ou identifiées comme telles.

En revanche, l'article 40, alinéa 2, du code de procédure pénale impose à tout fonctionnaire ou agent public d'informer, sans délai, le procureur de la République de tout crime ou délit dont il a connaissance dans l'exercice de ses fonctions.

## ARTICLE 6 – COMMUNICATION ELECTRONIQUE

### 1. Messagerie électronique

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

#### 6.1.1. Adresse électronique

L'institution s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. Elle est à utiliser pour tout échange professionnel permettant d'établir une communication interne ou externe entre les différents utilisateurs, suivant les standards techniques en vigueur sur les réseaux de communication numérique.

Les adresses mails peuvent prendre différentes formes principales :

- Nominative pour les personnels exerçant leurs activités en région académique : *<prenom.nom>[@]ac-rennes.fr* avec un chiffre si homonymie
- Nominative pour les personnels exerçant leurs activités à l'administration centrale : *<prenom.nom>[@]education.gouv.fr*
- Non nominatives pour les adresses fonctionnelles ou organisationnelles : *<fonction ou structure>[@]ac-rennes.fr* ou *<prefixe>.<fonction ou structure>[@]ac-rennes.fr*

Cette adresse est référencée dans l'annuaire interne de la Région académique. L'accès aux services offerts peut avoir lieu à partir de tout type de terminaux fournis par la Région académique. L'adresse électronique nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.

#### 6.1.2. Contenu du message

Tout message est réputé professionnel sauf s'il comporte dans son objet une mention particulière et explicite indiquant son caractère privé<sup>2</sup> ou bien s'il est stocké dans un espace privé de messages ou de données.

<sup>2</sup> Dossier mentionnant "PERSONNEL" ou "PRIVE"

Les démarches commerciales ou publicitaires, politiques ou religieuses, contraires aux principes de neutralité et de laïcité du service public de l'éducation sont interdites. De même, sont interdits les messages comportant des contenus à caractère illicite.

### **6.1.3. Émission et réception du message**

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

L'utilisation de listes de diffusion institutionnelles relève de la responsabilité de l'institution et de l'utilisateur qui doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés. L'utilisation de ces listes est réservée à un usage strictement professionnel.

Il veille également à ne pas émettre d'informations sensibles ou confidentielles. En cas de nécessité liée à ses fonctions, il devra alors s'assurer, avant toute émission, d'utiliser les outils de chiffrement prévus par l'institution.

Il est rappelé que la messagerie n'a pas vocation à servir pour le partage des documents ou pour l'envoi de fichiers volumineux. Des espaces de partage sont mis à disposition pour le stockage et un service numérique est disponible pour l'envoi de données volumineuses.

Il est rappelé qu'en application d'une directive du Premier ministre constante depuis 2013, le renvoi automatique d'une messagerie professionnelle vers une messagerie personnelle est à proscrire.

### **6.1.4. Stockage et archivage des messages**

Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles dans le cadre de son activité professionnelle.

Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet. La mention « privé » sera portée par les données relevant de la vie privée. Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur relevant de sa vie privée. En l'absence de désignation explicite du caractère privé, les données sont présumées avoir un caractère professionnel.

L'utilisateur sera informé par une notification automatique lorsque son taux d'utilisation de la boîte dépassera 90%.

### **6.1.5. Mesures de sécurité sur la messagerie**

La Région académique garantit la protection et la disponibilité du service de messagerie ainsi que du filtrage des courriers indésirables. La taille d'un message est limitée à 10 Mo.

- Le service de messagerie doit être sécurisé et pour cela, seul les protocoles sécurisés (smtps et imaps) doivent être utilisés.
- Toute pièce jointe potentiellement dangereuse (exécutable, macros...) sont détruites avant l'arrivée dans la boîte de l'utilisateur.
- Tout message considéré comme infecté par un virus est détruit sans notification.
- Tout message douteux est stocké dans le dossier « SPAM » de votre messagerie s'il n'est pas détruit par le serveur de messagerie à son arrivée.

Toute boîte impliquée dans un envoi de SPAM ou de PHISHING est systématiquement bloquée. L'utilisateur doit alors faire une demande à la plateforme d'assistance AMIGO pour la réactiver en changeant obligatoirement son mot de passe.

L'institution déploie un dispositif antivirus et un dispositif « antispam » qui contribuent à éviter la propagation des virus et bloquent, au mieux des possibilités qu'offre la technique, les messages non sollicités.

Une sauvegarde de l'ensemble de la messagerie académique est opérée quotidiennement pour permettre une reprise d'activité en cas d'incident. Cette sauvegarde ne permet cependant pas la restauration individuelle d'une boîte ou de son contenu qui aurait été perdu accidentellement. En conséquence aucune demande de restauration de boîte nominative ou fonctionnelle ne pourra être réalisée.

#### **6.1.6. Préconisations d'utilisation de la messagerie électronique nominative professionnelle**

L'accès à la messagerie nominative professionnelle peut s'effectuer de tout poste informatique disposant d'un accès à Internet, y compris du domicile.

Dans le respect des normes nationales, les boîtes de la messagerie nominative du ressort de la Région académique de Rennes font partie du domaine « ac-rennes.fr ».

Il convient de rappeler que quels que soient le lieu et le mode d'accès à la messagerie nominative professionnelle, les règles prévues par la présente charte s'appliquent intégralement.

En cas de problème technique, il convient de s'adresser au service d'assistance via le guichet unique (<http://assistance.ac-rennes.fr>).

En cas de cessation de fonction (mutation, départ à la retraite, etc.) entraînant une mise en position de l'agent en « fin de fonction » au sens de la gestion des ressources humaines, la boîte aux lettres nominative professionnelle est maintenue pendant une durée de 6 mois minimum. Deux vérifications sur la fin de fonction dans l'année scolaire sont réalisées. Une notification est envoyée aux agents concernés leur laissant 1 mois pour anticiper la suppression de leur compte de messagerie.

Cette durée peut être réduite à la demande motivée du responsable hiérarchique ou de l'intéressé. Ce délai permet à l'utilisateur d'avertir les correspondants du changement d'interlocuteur et d'assurer la continuité du service notamment par le transfert des messages reçus au titre de sa fonction précédente.

## **2. Internet**

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension Intranet) constitue l'un des éléments d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'institution.

Sur le lieu de travail, Internet est un outil réservé à un usage professionnel (administratif et pédagogique) avec un usage résiduel privé possible dans le respect de la législation en vigueur. Si une utilisation résiduelle privée, à condition d'être raisonnée, peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'administration sont présumées avoir un caractère professionnel. L'administration peut les rechercher aux fins de les identifier.

Au-delà des dispositions légales en vigueur, la consultation de sites contraires à la mission éducative de l'institution est interdite.

L'Institution 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 et des heures d'accès correspondantes dans le cadre d'une enquête administrative ou judiciaire.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution. L'utilisateur est informé des risques et des limites inhérents à l'utilisation d'Internet par le biais d'actions de formation ou de campagnes de sensibilisation.

### **6.2.1 Publications sur les sites académiques et intranet de l'institution**

Toute publication de pages d'information sur les sites internet ou intranet de l'institution doit être, au préalable, validée par un directeur de publication nommément désigné, dans le respect du droit d'auteur et de la propriété intellectuelle dans les publications rappelé dans l'article 6.

Aucune publication de pages d'information à caractère privé (pages privées ...) sur les ressources du système d'information de l'institution n'est autorisée.

### **6.2.2 Téléchargements**

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

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

## **ARTICLE 7 – TRACABILITÉ**

L'institution est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées.

Ces journaux sont consultables par les personnes juridiquement responsables (Recteur ou chefs d'établissement) en cas de constat d'infraction. Les données de ces journaux d'accès sont conservées pendant 1 an conformément à la loi en vigueur.

Les journaux d'accès font l'objet d'analyse statistique dans le but d'améliorer le service rendu. Dans le cadre de cette analyse, la constatation d'un usage délictueux ou criminel devra faire l'objet d'un signalement.

Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent en aucun cas divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions sauf en situation de réquisition judiciaire ou d'enquête administrative. Dès lors que ces informations sont couvertes par le secret des correspondances ou identifiées comme telles, elles relèvent de la vie privée de l'utilisateur.

## **ARTICLE 8 – PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL**

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite «Loi Informatique et Libertés» relative à la protection des données personnelles, en particulier lors de la création de fichiers auxquelles l'institution elle-même a l'obligation de se conformer, modifiée par la loi n° 2018-493 du 20 juin 2018 consécutivement à l'entrée en vigueur du Règlement Général sur Protection des Données.

Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès, de rectification, d'effacement, d'opposition, de limitation et de portabilité relatif à l'ensemble des données le concernant, y compris les données personnelles portant sur l'utilisation des systèmes d'Information.

Sauf mention particulière, ce droit s'exerce auprès du responsable du traitement.

Le non-respect des règles établies ou rappelées par la charte pourra donner lieu à la suspension de l'accès au service et à des sanctions de nature disciplinaires, indépendamment d'éventuelles sanctions pénales listés Article 8.

## ARTICLE 9 – RÈGLEMENT DES LITIGES

Si des difficultés surviennent entre les parties à l'occasion de l'interprétation ou de l'exécution de la présente charte, une solution amiable sera d'abord recherchée. A défaut d'accord, le litige sera déféré, par la partie la plus diligente, au Tribunal Administratif de Rennes.

Sont ainsi notamment (mais pas exclusivement) interdits et pénalement sanctionnés :

- l'atteinte à la vie privée d'autrui ;
- la diffamation et l'injure ;
- la provocation de mineurs à commettre des actes illicites ou dangereux, le fait de favoriser la corruption d'un mineur, l'exploitation à caractère pornographique de l'image d'un mineur, la diffusion de messages à caractère violent ou pornographique susceptibles d'être perçus par un mineur ;
- l'incitation à la consommation de substances interdites ;
- la provocation aux crimes et délits et la provocation au suicide, la provocation à la discrimination, à la haine notamment raciale, ou à la violence ;
- l'apologie des crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité ; la négation de crimes contre l'humanité ;
- la contrefaçon de marque ;
- la reproduction, représentation ou diffusion d'une œuvre de l'esprit (par exemple : extrait musical, photographie, extrait littéraire, ...) ou d'une prestation de droits voisins (par exemple : interprétation d'une œuvre musicale par un artiste, phonogramme, vidéogramme, programme d'une entreprise de communication audiovisuelle) en violation des droits de l'auteur, du titulaire de droits voisins et/ou du titulaire des droits de propriété intellectuelle ;
- les copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle.

## ARTICLE 10 – ENTRÉE EN VIGUEUR DE LA CHARTE

La charte a valeur de règlement intérieur pour ce qui concerne l'usage du système d'information.

Elle entre en vigueur dans toute la Région académique et pour tous les personnels à compter de sa publication sur les sites intranet et internet de la Région académique le 14 mai 2025.

## ARTICLE 11 – DISPOSITIONS FINALES

Dans l'hypothèse où des dispositions législatives ou réglementaires ou qu'une circulaire ministérielle viendraient à définir et préciser les conditions d'utilisation des technologies de l'information et de la communication par les personnels, la Région académique procéderait aux adaptations éventuellement nécessaires.

Fait à Rennes, le 14 Mai 2025

La Rectrice de la Région académique Bretagne  
Chancelière des universités

Hélène INSEL