RÉGION ACADÉMIQUE
LA RÉUNION

Liberté
Égalité
Fraternité

CHARTE DES USAGES
DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE

RÉGION ACADÉMIQUE
LA RÉUNION

Liberté
Égalité
Fraternité

CHARTE RÉGISSANT LES USAGES DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE PAR LES PERSONNELS DE LA RÉGION ACADÉMIQUE DE LA RÉUNION

Version juin 2025

Sommaire

Préambule

Par "système d'information" s'entend l'ensemble des ressources matérielles (ordinateurs, terminaux mobiles et nomades, périphériques actifs,...), logicielles, applications, services en ligne, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'Institution.

Par «institution», s'entend tout service (administration centrale, rectorat et sites déconcentrés, inspections et délégations académiques) ou établissements d'enseignement public du premier et du second degré relevant du ministère de l'Éducation nationale.

Par «utilisateur», s'entend tout personnel ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information, quel que soit son statut.

Ainsi est notamment désigné :

- tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'éducation ;
- tout prestataire[1] ayant contracté ou tout partenaire ayant conventionné 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 qui s'imposent, notamment le respect des règles visant à assurer la sécurité (ex : Politique de Sécurité des Systèmes d'Information de l'État[2] et de l'académie de la région Académique de La Réunion[3], Règlement Général sur la Protection des Données – RGPD[4], posture VIGIPIRATE[5],....), 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 s'engagent à respecter : elle précise les droits et devoirs de chacun.

La charte peut être complétée par des guides d'utilisation définissant les principales règles et pratiques d'usage.

Engagements de l'Institution

L'Institution met en place différentes mesures pour assurer la sécurité du système d'information et la protection des utilisateurs notamment en matière d'authentification, de disponibilité et d'intégrité, de confidentialité et de traçabilité.

L'institution met à disposition de chaque personnel une identité numérique professionnelle donnant accès à ses données de carrière et des données générées dans le cadre de sa pratique professionnelle, ainsi qu'aux systèmes d'information de l'Éducation Nationale. Lorsqu'un agent quitte l'académie, son identité numérique ainsi que sa messagerie peuvent être supprimés dans un délai qui respecte à la fois les nécessités de service et son droit à l'oubli. (Actuellement 12 mois, mais cela peut varier en fonction des directives ministérielles).

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

---

1 Le contrat devra prévoir expressément l'obligation de respect de la charte.
2 https://cyber.gouv.fr/cadre-de-gouvernance-de-la-securite-numerique-de-letat-pssie
3 https://portail.ac-reunion.fr/ladoclela/shelves/cybersecurite

4 Règlement entré en application le 25 mai 2018 : https://www.cnil.fr/fr/reglement-europeen-protection-donnees
5 http://www.sgdsn.gouv.fr/plan-vigipirate/

Engagements de l'utilisateur

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] et du devoir de réserve dans ses communications effectuées avec son identité numérique professionnelle à destination de l'ensemble des acteurs interagissant avec l'Institution (messagerie, réseaux sociaux...).

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

Les usages des ressources informatiques non conformes aux préconisations de la présente charte peuvent être regardés comme des fautes professionnelles susceptibles d'entraîner pour l'utilisateur une suspension conservatoire des outils mis à disposition, des sanctions disciplinaires, sans préjudice d'éventuelles actions pénales ou civiles à son encontre.

Dans tous les cas, l'utilisation doit être conforme à l'ordre public et aux lois en vigueur, et ne doit en aucun cas compromettre l'intégrité, la réputation ou l'image de l'administration.

Article I. 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.

La présente charte s'applique à tous les types d'usage, depuis les locaux des entités ou dans le cadre d'un usage dit « nomade », indépendamment du moyen utilisé pour assurer le traitement ou le stockage de l'information et indépendamment du lieu où l'information est traitée ou stockée.

Les usages relevant de l'activité des organisations syndicales sont régis par une charte spécifique[7].

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

Section 2.01 - Utilisation professionnelle / personnelle

Les moyens informatiques et outils numériques sont des supports de travail ouverts à des usages professionnels, d'ordre administratif, pédagogique ou éducatif et peuvent constituer un support de communication, de production ou de collaboration personnelle.

L'utilisation résiduelle du système d'information professionnel à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. 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'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.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère personnel dans un espace de données prévues explicitement[8] à cet effet ou en mentionnant le caractère privé sur la ressource. La sauvegarde régulière des données à caractère personnel incombera à l'utilisateur ainsi que leur suppression.

---

6 Ensemble des règles et des devoirs qui régissent une profession, la conduite de ceux qui l'exercent, les rapports entre l'ensemble des acteurs.

7 Circulaire n° 2012-080 du 20-4-2012

8 Cet espace devra être nommé [PERSONNEL-PRIVE]

Section 2.02 - Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service, l'utilisateur en cas d'absence informe sa hiérarchie des modalités[9] permettant l'accès aux ressources mises spécifiquement à sa disposition[10] .

En cas d'absence de l'agent, l'institution peut être amenée à accéder à ses données professionnelles et aux modalités[11] permettant la continuité de service. Dans la mesure du possible, l'institution s'efforcera d'informer l'agent au préalable. Si une notification préalable n'est pas possible, l'agent sera informé dès que possible après l'accès aux données.

En cas d'absence non planifiée et pour des raisons exceptionnelles, si un utilisateur se trouve dans l'obligation de communiquer ses codes d'accès[12] au système d'information, il doit procéder, dès que possible, au changement de ces derniers ou en demander la modification à l'administrateur.

L'Institution ne peut, sans violer le droit au respect de la vie privée, consulter les messages électroniques et les fichiers portant explicitement la mention du caractère privé par l'indication **[PERSONNEL-PRIVE]** sauf risque ou événement particulier[13].

Seule une personne disposant des compétences techniques et dûment habilitée pour utiliser les identifiants administrateurs peut délivrer les accès aux données de l'agent absent.

Dans l'intérêt du service et des utilisateurs, l'Institution recommande d'utiliser les espaces partagés qu'elle leur met à disposition (partages réseau, outils de synchronisation et de partage de données, Environnements Numériques de Travail...) pour y stocker leurs données professionnelles, afin de faciliter la transmission des informations en cas d'arrivée/départ, perte ou vol.

L'utilisateur est responsable de son espace de données à caractère privé. 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'institution ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles ayant été définies en amont avec le responsable hiérarchique au sein de l'institution.

Section 2.03 – Télétravail et travail à distance

Le télétravail désigne une forme d'organisation du travail dans laquelle, un acte professionnel qui aurait pu être exécuté dans les locaux de l'administration est effectué par un agent hors de ces locaux, en utilisant les technologies de l'information et de la communication. Il se pratique au domicile de l'agent – entendu comme le lieu de sa résidence habituelle – ou, le cas échéant, dans des locaux professionnels (validés par l'Institution) distincts de son lieu d'affectation.

Le télétravailleur bénéficie des mêmes droits et est soumis aux mêmes obligations que les agents travaillant sur site.

Il s'engage également à respecter la confidentialité des informations détenues ou recueillies dans le cadre de son activité et à veiller à ce qu'elles ne soient pas accessibles à des tiers.

Section 2.04 – Eco-sobriété numérique

La charte d'usage du numérique reflète un engagement commun entre l'Institution et les utilisateurs pour adopter des pratiques numériques responsables et durables.

---

9 À titre d'exemple, en cas de départ ou d'absence prolongée provoquant un blocage fonctionnel du service, les droits devront être retirés à la personne absente, et ajoutés à la personne remplaçante.

10 Ces dispositions peuvent être adaptées en fonction de la spécificité des activités exercées, notamment lorsque des données présentent un caractère de confidentialité ou de secret avéré.

11 À titre d'exemple, en cas de départ ou d'absence prolongée provoquant un blocage fonctionnel du service, les droits pourront être retirés à la personne absente, et ajoutés à la personne remplaçante.

12 Identifiants, mots de passe, dispositifs d'accès logique ou physique (carte à puce, clés de sécurité ...).

13 Autorité judiciaire via réquisition, perquisition ou saisie de donnée

de la part de l'Institution :

- Favoriser les achats respectueux de l'environnement, favorisant les produits écocertifiés et reconditionnés ;
- Optimiser l'efficacité énergétique ;
- Adopter la virtualisation et la mutualisation de ressources ;
- Prolonger la durée de vie des équipements grâce à des programmes de maintenance et de réparation ;
- Encourager la réutilisation et le recyclage des équipements en fin de vie ;
- Favoriser l'utilisation d'espaces de stockage partagés pour éviter la duplication inutile des données.

de la part de l'utilisateur :

- Prendre soin des équipements pour prolonger leur durée de vie et demander des réparations si nécessaire ;
- Privilégier les équipements reconditionnés ou de seconde main ;
- Réduire les e-mails non essentiels et éviter les pièces jointes volumineuses ;
- Nettoyer régulièrement les boîtes de réception et les espaces de stockage en supprimant les fichiers inutiles ;
- Éteindre les équipements lorsqu'ils ne sont pas utilisés (ordinateurs, écrans,.) ;
- Désactiver les fonctionnalités énergivores quand elles ne sont pas nécessaires ;
- Participer activement aux programmes de sensibilisation et de formation proposés par l'Institution ;
- Limiter l'usage de services de « streaming » et privilégier le téléchargement ;
- Utiliser les « services en ligne » avec parcimonie et stocker localement les données non critiques.

Article III. Principes de sécurité

Section 3.01 - Règles de sécurité applicables

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

L'utilisateur est informé que les codes et moyens d'accès logiques et physiques (clés, badge magnétique, identifiant/mot de passe, clés OTP, etc.) constituent des mesures de sécurité destinées à éviter tout agissement malveillant ou abusif.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est confiérée. La sécurité des systèmes d'information lui impose :

- de respecter les consignes de sécurité, en particulier les règles concernant la gestion des mots de passe et des codes d'accès aux services numériques [14] ;
- de se connecter et de s'authentifier sur le réseau de l'institution en utilisant uniquement les moyens ou méthodes sécurisés mis en place à cet effet par l'institution ;
- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers (sauf cas prévus en section 2.02) ;
- de respecter la gestion des accès, en particulier ne pas utiliser le badge ou les codes d'accès d'un autre utilisateur ni chercher à les connaître pour les seconds.

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

de la part de l'institution :

- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes dûment habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie (Cf. section 2.02), conformément à la politique des moindres privilèges (en limitant les accès aux seules informations et fonctions utiles à chacun);

[14] Politique des mots de passe de la région académique sous directive nationale : https://portail.ac-reunion.fr/ladoclela/books/application-changement-de-mot-de-passe

- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

de la part de l'utilisateur :

- s'interdire d'accéder ou de tenter d'accéder à tout ou partie du système d'information pour lesquelles il n'a pas reçu d'habilitation explicite[15] ;
- 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'Institution, des logiciels ou progiciels qui ne respecteraient pas les directives du service informatique et/ou les droits de licence et/ou CGU ;
- ne pas modifier, détruire des logiciels sur le matériel de l'Institution et leur paramétrage sans autorisation ;
- verrouiller (ou éteindre) son ordinateur dès que l'on quitte son poste de travail ;
- se conformer aux dispositifs mis en place par l'Institution pour lutter contre les virus et les attaques par programmes informatiques ;
- L'utilisation de périphériques amovibles (comme les clés USB) sur du matériel professionnel doit être limitée au strict nécessaire et faire l'objet d'une surveillance rigoureuse. Il est essentiel de suivre les procédures établies par l'Institution, notamment en obtenant l'accord du supérieur hiérarchique et en respectant les mesures de sécurité, telles que le chiffrement des données ;
- La connexion de matériel professionnel ou personnel à un réseau externe notamment en déplacement doit respecter les bonnes pratiques du nomadisme, notamment le guide[16] de l'ANSSI[17] et les recommandations de la CNIL[18].

Section 3.02 Terminaux[19] professionnels / personnels

(a) L'agent est doté d'un terminal par l'académie ou la collectivité territoriale

L'usage de terminaux professionnels est dans ce cadre imposé, notamment en situation de télétravail. La connexion de terminaux personnels[20] aux réseaux locaux de l'Institution ou à distance (ex : liaison filaire « RJ45 » ou « VPN ») n'est pas autorisée lorsque l'agent est doté d'un terminal par l'académie ou la collectivité territoriale.

Il est interdit d'installer des applications non validées par l'institution (notamment les applications récréatives...).

(b) L'agent n'est pas doté d'un terminal par l'académie ou la collectivité territoriale

En cas d'absence de dotation de matériels dédiés aux usages professionnels par l'académie ou la collectivité territoriale, les agents peuvent être amenés à connecter leurs terminaux personnels aux réseaux locaux.

Cas d'usages non autorisés via des terminaux personnels :

- la connexion aux réseaux administratifs des établissements ;
- la connexion aux réseaux filaires des services académiques.

En cas de non-respect de ces consignes, les sanctions encourues sont décrites ci-après (cf l'article VIII).

---

15 Les sanctions pour les intrusions sur les systèmes automatisés de traitement de données sont définies dans le Code pénal français, principalement aux articles 323-1 à 323-3

16 https://cyber.gouv.fr/publications/bonnes-pratiques-lusage-des-professionnels-en-deplacement

17 Agence Nationale de la Sécurité des Systèmes d'Information : https://cyber.gouv.fr/

18 Commission Nationale de l'Informatique et des Libertés : https://www.cnil.fr/

19 Par « terminaux » s'entendent tous types de matériels : ordinateur fixe/portable, tablette, smartphone, ...

20 Terminaux désignés sous les acronymes BYOD (Bring your Own Device) ou AVEC (Apportez Votre Équipement personnel de Communication).

Après accord de l'autorité compétente (Rectorat, Commune, Département, Région) les autres cas d'usage sont autorisés.

Ces terminaux doivent en complément respecter les recommandations suivantes :

- disposer d'un système d'exploitation à jour : dans cette optique, l'utilisateur doit seulement s'assurer que les mises à jour automatiques sont bien activées sur son terminal, et s'assurer régulièrement de leur bonne installation ;
- disposer de tout moyen nécessaire à sa sécurité, tels que anti-virus, EDR[21] ;
- disposer des dernières mises à jour des autres applications mises à disposition par l'institution ou la collectivité territoriale, lorsqu'elles le sont également pour une installation sur un terminal personnel ;
- Privilégier un compte de moindre privilège ne disposant pas de droits d'administration pour l'utilisation courante en cas de raccordement au système d'information.
- Les terminaux mobiles de type ordinateurs portable devraient être chiffrés afin d'éviter les divulgations de données en cas de perte ou de vol.

Section 3.03 - Devoirs de signalement et d'information

L'institution doit porter à la connaissance de l'utilisateur les éléments susceptibles de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information et de communication en intégrant les nouveaux systèmes de communication type TOIP (voix sur internet protocole), chat (messagerie instantanée), ...

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté, de toute perte ou vol de matériel ou de toute anomalie découverte telle une intrusion dans le système d'information, etc. Il signale également toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation en déclarant un incident de sécurité sur le portail d'assistance académique (FILAOS) ou auprès de la collectivité territoriale en charge de son école ou de son établissement.

Section 3.04 - Mesures de contrôle de la 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 ;
- qu'une maintenance à distance est précédée d'une information ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée, et le cas échéant mise en quarantaine.

Dans le respect de la législation en vigueur, l'Institution informe l'utilisateur que l'administration du système d'information donne lieu, entre autres, à :

- une surveillance et un contrôle à des fins statistiques ;
- une traçabilité réglementaire ou fonctionnelle des actions (cf article V) ;
- une détection des abus ;
- un filtrage des flux ;
- une gestion de terminaux via un outil tel qu'un « Mobile Device Management »[22];

Les personnels en charge de ces opérations de contrôle des systèmes d'information sont soumis entre autres au secret professionnel,

---

[21] EDR : Surveillance et réponse aux menaces en temps réel sur les points finaux (ordinateurs, serveurs, appareils mobiles) pour détecter et neutraliser les comportements suspects.

[22] Mobile Device Management ou en français « gestion des appareils mobiles »

Article IV. Communications électroniques

Section 4.01 Messagerie électronique

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

(a) Adresses électroniques

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.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative. Cette adresse nominative est l'adresse professionnelle de l'agent.

La gestion de toute adresse électronique nominative[23] attribuée à un utilisateur relève de sa responsabilité.

Une adresse électronique, partagée, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs, celle-ci sera sous la responsabilité d'un ou plusieurs référents.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe «d'utilisateurs», relève de la responsabilité de l'Institution.

(b) Contenu des messages électroniques

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur par le fournisseur de service de messagerie.

Sont interdits les messages comportant des contenus à caractère illicite, quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui.

L'utilisation de la messagerie professionnelle par les organisations syndicales depuis les systèmes d'information de l'Institution est régie par la charte relative aux usages syndicaux.

(c) Émission et réception des messages

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

Il doit veiller à ce que la diffusion 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.

(d) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles[24] 1369-1 à 1369-11 du Code civil.

L'utilisateur doit, en conséquence, être vigilant quant à la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

(e) 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 en tant qu'éléments de preuve, avec les moyens mis à sa disposition.

---

23 Pour exemple, adresse administrative de la forme prenom.nom@ac-reunion.fr ou adresse pédagogique de la forme prenom.nom@i<eple>xxxx.fr

24 Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne.

À ce titre, il doit notamment se conformer aux règles définies dans la présente charte et, le cas échéant, dans le ou les guides d'utilisation établi(s) par le service ou l'établissement.

(f) Règles du bon usage de la messagerie

L'ensemble des utilisateurs de l'institution doivent respecter les règles d'usage de la messagerie suivantes :

- faire un usage raisonné de la messagerie conformément à la démarche de sobriété numérique (par exemple utiliser un service de transfert de fichier volumineux[25]) ;
- en fonction de la sensibilité de l'information ou de présence de données à caractère personnel, il peut être nécessaire d'appliquer un chiffrement[26]. Le code secret sera adressé aux destinataires pour un autre canal de communication ;
- Une clause de confidentialité peut être insérée dans le cartouche de signature comme suit : *Ce message est confidentiel et réservé aux destinataires ; toute diffusion non autorisée est interdite. Si reçu par erreur, détruisez-le et avertissez l'émetteur*
- ne pas diffuser de messages de type canulars, chaînes, escroquerie par hameçonnage (phishing), jeux, etc. ;
- ne pas utiliser l'adresse électronique professionnelle dans un contexte non professionnel, en particulier, ne pas l'utiliser sur des sites internet (groupes de discussion (chats), commerce, forums, blogs, etc.), sans rapport avec l'activité professionnelle ;
- éviter l'utilisation d'adresses de messageries personnelles dans un contexte professionnel ;
- pour des raisons de sécurité et de confidentialité, l'utilisation d'une boîte à lettres professionnelle à titre privé n'est pas recommandée ;
- s'assurer, à chaque envoi de données, en particulier sensibles, que la liste de diffusion ne comporte pas de destinataire inapproprié ;
- si vous recevez un message inhabituel ou suspect, adoptez une attitude prudente : évitez d'ouvrir le message, de cliquer sur les liens, de télécharger les pièces jointes ou de répondre à l'expéditeur ;
- prévenir l'assistance informatique : **alerte_mail@ac-reunion.fr** en cas de doute, et même après l'ouverture d'un message ou d'un clic sur un lien qui s'avère a posteriori douteux ;
- privilégier la messagerie pédagogique (celles proposées par l'ENT) pour les communications avec les élèves et les responsables légaux, la messagerie professionnelle devant être réservée aux communications entre pairs ou avec l'institution ;
- Une clause de respect et au droit à la déconnexion peut être insérée dans le cartouche de signature comme suit : *Si ce message vous parvient en dehors des jours ou des heures de travail, il ne requiert pas de réponse avant le retour de ces conditions.*

Section 4.02 – 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 essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'institution.

L'utilisation de sites internet institutionnels pour consulter, traiter, ou stocker des informations professionnelles doit être privilégiée. A contrario, certains critères de sécurité doivent être vérifiés (localisation des données, types de données traitées, transferts de données, chiffrement...).

L'Institution ou les collectivités territoriales met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

---

[25] Type filesender ou France transfert.

[26] https://portail.ac-reunion.fr/ladoclela/shelves/cybersecurite

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques) : il peut constituer le support d'une communication privée telle que définie en section 2.01 dans le respect de la législation en vigueur.

En complément des dispositions légales en vigueur et en considération de la mission éducative et de protection des mineurs assumée par l'Institution, l'accès volontaire, depuis ses locaux, à des contenus attentatoires à la dignité humaine, contraires aux bonnes mœurs ou aux valeurs éducatives, est strictement interdit.

(a) Publications sur les sites internet et intranet de l'Institution

Toute publication de pages d'information sur les sites internet ou intranet de l'Institution[27] doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication de pages d'information à caractère privé (pages privées ...) sur les ressources du système d'information de l'institution n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le service ou l'établissement.

(b) Sécurité des accès à Internet

L'Institution se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder, dans un cadre légal, au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'Institution. 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'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.

(c) Limitation des suites collaboratives en ligne d'éditeurs états-uniens ou non-européens dans les écoles et les établissements publics

Conformément à la priorité donnée à la protection des données à caractère personnel des élèves et des personnels et à la volonté de la France de privilégier des solutions souveraines, le ministère continue de proscrire tout déploiement de suites collaboratives en ligne d'éditeurs états-uniens ou non-européens dans les écoles et les établissements publics.[28]

(d) Les réseaux sociaux

Concernant les réseaux sociaux, il convient de prendre connaissance des recommandations du collège déontologique de l'Éducation nationale, notamment la première concernant les trois dimensions : sphère publique, sphère privée et sphère professionnelle.

(e) Outils d'intelligence générative

L'intelligence générative, ou IA générative est une technologie qui permet à des systèmes informatiques de produire automatiquement du contenu, tel que du texte, des images, ou des sons, à partir de grandes quantités de données.

Leur usage doit être encadré pour prévenir les dérives potentielles et notamment veiller à ne pas transmettre des informations contenant des données personnelles et/ ou sensibles et/ou stratégique. En effet, de nombreux moteurs d'I.A utilisent les données fournies dans les « prompts » pour affiner ou améliorer leurs capacités. Les outils utilisés doivent être compatibles avec la réglementation européenne « AI Act». [29]

L'utilisation devra également être conforme au cadre d'usage I.A qui sera mis en forme par la Direction du Numérique Educatif à la rentrée de septembre 2025.

---

27 À partir des ressources informatiques mises à la disposition de l'utilisateur.

28 Note direction du numérique éducatif du 28 février 2025

29 IA. Acte https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1689

Section 4.03 – 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 (cf l'article VI.)

L'institution se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux et/ou présentant un risque pour la sécurité des systèmes d'information (virus, codes malveillants ...) susceptibles d'altérer le bon fonctionnement du système d'information de l'Institution), conformément à la démarche de sobriété numérique.

Article V. Traçabilité

L'Institution est dans l'obligation légale de mettre en place un système de journalisation[30] des accès Internet, de la messagerie électronique et des données échangées.

L'Institution se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes d'information.

Article VI. Propriété intellectuelle

L'Institution rappelle que l'utilisation des 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 utilisateur doit:

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

Les développements[31] informatiques effectués par un agent de l'État dans le cours de l'exercice de ses fonctions, s'inscrivant dans le domaine des activités du service, ou grâce à la connaissance ou l'utilisation des techniques ou de moyens spécifiques au service, ou de données procurées par celui-ci, sont réputés d'appartenir à l'État.

Article VII. Activités de traitements de données à caractère personnel

En application des dispositions du règlement (UE) 2016/679 du Parlement Européen et du Conseil 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 (RGPD) et la Loi n° 2018-493 du 20 juin 2018 et son décret d'application l'institution ainsi que les utilisateurs s'engagent à respecter les règles légales relatives à la protection des données personnelles.

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.

Les traitements de données à caractère personnel mis en œuvre dans l'académie doivent préalablement faire l'objet d'une inscription aux registres des traitements de l'EPLE, du premier degré ou des services académiques et régionaux[32].

---

[30] Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur.

[31] https://www.cnil.fr/fr/guide-rgpd-du-developpeur

[32] Les registres sont dématérialisés via l'application RADIO (Registre des Activités de Données Individuelles de l'Organisation), accessible sur l'environnement numérique de travail Metice dans la rubrique « Ressources et outils

En conséquence, tout personnel souhaitant procéder à la création de traitement de données à caractère personnel devra en informer son supérieur hiérarchique et le responsable de traitement de structure.

Par ailleurs, conformément aux dispositions de cette loi, chaque personne dispose de droits relatifs à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'Information.

Les demandes relatives aux traitements de données à caractère personnel mis en œuvre au sein de l'académie peuvent être adressées, selon les cas, au référent RGPD de votre structure (si elle en est pourvue) ou au délégué académique à la protection des données

- par courriel : dpd@ac-reunion.fr
- par courrier postal adressé au :
  Secrétariat Général – Déléguée académique à la protection des données
  Rectorat de La Réunion 24 Avenue Georges Brassens 97743 Saint-Denis Cedex 9
- par formulaire de contact https://www.ac-reunion.fr/espace-contact

Une annexe détaillée et spécifique à la politique de protection des données de l'académie au RGPD sera établie et disponible sur le site de l'académie.

Article VIII. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation établis par le service ou l'établissement, la « personne juridiquement responsable » pourra, sans préjuger des poursuites judiciaires ou procédures disciplinaires pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Par « personne juridiquement responsable », on entend : toute personne ayant la capacité de représenter l'institution (recteur, directeur académique, chef d'établissement, directeur d'établissement...).

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

Sont susceptibles d'être regardés comme abusifs tous comportements :

- visant à induire en erreur ou à outrepasser les mesures de sécurité mises en œuvre pour assurer le bon fonctionnement des services,
- ayant entraîné une consommation manifestement excessive, au regard des missions confiées à l'utilisateur, sur un ou plusieurs abonnements ou autres ressources mises à disposition,
- ayant entraîné la diffusion volontaire d'informations à des destinataires n'ayant aucun besoin légitime de connaître leur contenu,
- ayant entraîné la diffusion de données comportant des contenus à caractère illicite (notamment ceux attentatoires à vie privée d'autrui, diffamatoires ou relevant de l'injure, attentatoire à la liberté d'expression, de nature à provoquer des mineurs à commettre des actes illicites ou dangereux, faisant l'apologie du terrorisme, etc...),
- ayant entraîné le téléchargement, l'installation, ou l'utilisation sur le matériel de l'institution, de logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou dépourvus d'autorisation de sécurité délivrée la par l'académie.

Article IX. – Cas spécifique des usagers à privilèges

Tout usager disposant de droits ou de privilèges particuliers sur le système d'information en termes d'administration technique ou fonctionnelle est tenu à une confidentialité et une exigence déontologique accrue ainsi qu'une prudence dans ses actes de maintenance.

Tout personnel disposant de privilèges s'engage à respecter toutes les mesures de sécurité nécessaires à la protection des informations et au maintien de leur non-divulgation et leur confidentialité.
Il doit disposer d'une politique d'accès spécifique et renforcée (ex : OTP, Mot de passe à 16 caractères, ...)
Tout personnel disposant de privilèges s'engage à garder confidentielles et à ne pas divulguer à des tiers, toutes les informations, y compris à caractère privé, qui lui ont été révélées et dont il a eu connaissance dans le cadre de ses missions ou de son travail, quel qu'en soit le support (numérique, écrit, oral).
À cet égard, les personnels disposant de privilèges s'engagent à :
- veiller à ce que les tiers non autorisés n'aient pas connaissance de ces informations ;
- respecter l'obligation de réserve et le devoir de discrétion en usage au sein du ministère ;
- s'assurer de l'identité et des habilitations des utilisateurs dans son périmètre pour l'accès à tout ou partie d'éléments du système d'information, en liaison avec son responsable hiérarchique ;
- réaliser des actualisations d'habilitation régulières, en lien avec les responsables métiers, pour ajuster les accès en fonction des évolutions de missions ;
- préserver la confidentialité de leurs moyens d'identification (mots de passe, dispositifs d'authentification) ;
- garantir la transparence dans l'emploi d'outils de prise en main à distance ou toute autre intervention sur l'environnement de travail individuel de l'utilisateur ;
- signalé sans délai tout incident ou anomalie suspecte liée aux privilèges à l'autorité compétente (RSSI ou DSI).

Article X. Entrée en vigueur de la charte

La présente charte a valeur de règlement intérieur pour ce qui concerne l'usage des systèmes d'information et du numérique de la région académique de La Réunion et des différentes structures sous tutelle de l'Éducation Nationale dans la région académique de La Réunion.

Pour l'ensemble de la région académique de La Réunion, le présent document fait également l'objet d'une communication devant :

- le «conseil d'école des écoles publiques maternelles , élémentaires et primaires ;
- le «conseil d'administration» des établissements publics locaux d'enseignement (EPLE).

Cette charte a été présentée le 13 juin 2025 en comité social académique (CSA)

Cette charte prendra effet à compter de sa publication et communication.

Le recteur de région académique,
recteur d'académie

RECTORAT
ST DENIS - REUNION

Rostane MEHDI