

Règles définissant l'usage du système d'information de l'académie de Reims mis à disposition des personnels

➔ SOMMAIRE

Article I. Champ d'application page 4

Article II. Conditions d'utilisation des systèmes d'information..... page 4

Section 2.01 Utilisation professionnelle / privée..... page 4

Section 2.02 Continuité de service : gestion des absences et des départs..... page 4

Article III. Principes de sécurité..... pages 5 et 6

Section 3.01 Règles de sécurité applicables page 5

Section 3.02 Devoirs de signalement et d'information page 6

Section 3.03 Mesures de contrôle de la sécurité page 6

Article IV. Traçabilité..... page 7

Article V. Respect de la propriété intellectuelle page 7

Article VI. Respect de la loi informatique et libertés page 7

Article VII. Limitation des usages..... page 8

Article VIII. Entrée en vigueur des règles d'usage..... page 8

Article IX. Communication électronique pages 8 à 10

Section 4.01 Messagerie électronique..... pages 8 et 9

(a) Adresses électroniques page 8

(b) Contenu des messages électroniques..... page 8

(c) Émission et réception des messages..... page 9

(d) Statut et valeur juridique des messages page 9

(e) Fin de fonctions de l'utilisateur..... page 9

(f) Stockage et archivage des messages page 9

Section 4.02 Internet pages 9 et 10

(a) Publication sur les internet et intranet de l'institution..... page 10

(b) Sécurité..... page 10

Section 4.03 Téléchargements..... page 10

Article X. Diffusion des règles d'usage auprès des personnels page 10

Préambule

Le "système d'information" recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'institution.

L'informatique nomade, tels que les assistants personnels, les ordinateurs portables, les téléphones portables..., est également un des éléments constitutifs du système d'information.

Par "institution" il faut entendre tout service utilisant le système d'information de l'académie de Reims (à titre d'exemples : rectorat, direction des services départementaux de l'Éducation nationale, circonscription de premier degré, CIO, école, établissement public local d'enseignement).

Le terme d'"utilisateur" recouvre tout personnel ou prestataire ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du 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 ;
- tout prestataire*¹ ayant contracté, avec l'institution ou avec une collectivité territoriale ayant compétence partagée avec l'Etat 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.

Le présent document définit les règles d'usage et de sécurité que l'institution et l'utilisateur s'engagent à respecter : il précise les droits et devoirs de chacun. Il est accompagné d'un guide juridique qui rappelle les dispositions législatives et réglementaires en vigueur pour son application.

Engagements de l'institution

L'institution porte le présent document à la connaissance de l'utilisateur.

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

L'institution facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'institution est tenue de respecter l'utilisation résiduelle du système d'information à titre privé.

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*².

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

¹ Le contrat devra prévoir expressément l'obligation de respect des règles d'usage du système d'information.

² Notamment le secret médical dans le domaine de la santé.

Article I. Champ d'application

Les règles d'usage et de sécurité figurant dans le présent document s'appliquent à l'institution ainsi qu'à l'ensemble des utilisateurs.

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

Section 2.01 Utilisation professionnelle / privée

Les systèmes d'information (notamment par exemple, la messagerie, l'accès à internet) sont des outils de travail ouverts à des usages professionnels administratifs et pédagogiques.

Ils peuvent également constituer le support d'une communication privée dans les conditions décrites ci-dessous.

L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et demeurer raisonnable dans sa fréquence et dans sa durée : elle ne doit, notamment, pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service, et le surcoût qui en résulte pour l'institution doit demeurer négligeable au regard du coût global d'exploitation.

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 privé dans un espace de données prévu explicitement^{*3} à cet effet, ou en mentionnant le caractère privé sur la ressource^{*4}. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

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'administration ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies avec le responsable désigné, au sein de l'institution.

L'utilisation des systèmes d'information à titre privé doit respecter la législation et réglementation en vigueur.

Par ailleurs, eu égard à la mission éducative de l'institution, la consultation de sites de contenus à caractère pornographique depuis les locaux de l'institution est interdite.

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

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition.

³ Par exemple, cet espace pourrait être dénommé " Dossier à caractère privé Prénom NOM ".

⁴ Par exemple " Privé_nom_de_l_objet_NOM_Prénom ".

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 comptes d'accès qui lui sont confiés constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive des ressources du système d'information qu'il est habilité à utiliser. Cette mesure ne confère pas aux ressources protégées un caractère personnel.

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 exige de sa part le respect des consignes de sécurité relatives à la gestion de ses comptes d'accès :

- en garantir à tout moment le caractère personnel, incessible et confidentiel ;
- garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers ;
- ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

Il est notamment rappelé que l'usage qui est fait du système d'information au moyen d'un compte d'accès engage la responsabilité de l'utilisateur à qui ce compte a été confié.

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

> de la part de l'utilisateur :

- s'interdire d'accéder ou tenter d'accéder à des ressources du système d'information pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas connecter aux réseaux locaux académiques à vocation administrative^{*5} des matériels autres que ceux confiés ou autorisés par l'institution, ou aux autres réseaux institutionnels^{*6} des matériels autres que ceux confiés ou autorisés par le service ou l'établissement ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'institution des logiciels 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.

⁵ Réseaux du rectorat, des DSDEN et des circonscriptions d'IEN ; réseaux administratifs des EPLE, des CIO et des GRETA.

⁶ Notamment les réseaux pédagogiques des EPLE, des écoles, des CIO et des GRETA.

Section 3.02 Devoirs de signalement et d'information

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté, ou de toute anomalie découverte dans le système d'information. Il s'engage à signaler toute possibilité d'accès à une ressource ne relevant pas de son niveau d'habilitation qu'il aurait pu constater.

Section 3.03 Mesures de contrôle de la sécurité

L'utilisateur est informé :

- que pour effectuer la maintenance corrective 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 de l'utilisateur ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée, le cas échéant supprimée.

L'institution informe l'utilisateur que le système d'information donne lieu à une surveillance 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.

L'institution est dans l'obligation légale de mettre en place un système de journalisation^{*7} des accès Internet, de la messagerie et des données échangées.

Préalablement à cette mise en place, l'institution procédera, auprès de la Commission nationale de l'informatique et des libertés, à une déclaration, qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n° 78-17 du 6 janvier 1978 modifiée.

Les personnels chargés des opérations de contrôle 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 dès lors que ces informations sont couvertes par le secret des correspondances ou explicitement identifiées comme relevant de la vie privée de l'utilisateur.

En revanche, ils doivent communiquer ces informations aux autorités compétentes si elles sont constitutives d'un crime ou délit et tombent ainsi dans le champ de l'article^{*8} 40 alinéa 2 du code de procédure pénale.

⁷ Conservation des informations techniques de connexion telles que la date et l'heure d'accès, le site consulté, l'adresse IP et le cas échéant l'identité de l'utilisateur.

⁸ Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la république de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.

Article IV. Traçabilité

En matière de conservation de traces, la loi impose de conserver les traces de connexion. Cette obligation ne s'applique pas uniquement aux opérateurs de télécommunication comme défini dans la loi du 21 juin 2004 ou Loi pour la Confiance dans l'Economie Numérique (LCEN).

Les traces de connexion des personnels qui utilisent les dispositifs de communication mis à disposition par l'Académie de Reims sont donc enregistrées et conservées pendant une durée d'un an.

Il est également précisé dans le Code des Postes et des Communications Electroniques article L34-1 que :

Sont également tenues à l'obligation de conservation des données de connexions les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès réseau, y compris à titre gratuit.

Il est à noter que la durée de conservation de ces traces est fixée à 1 an maximum par les articles L34-1 et R10-13 du Code des Postes et des Communications Electroniques.

Article V. Respect de la propriété intellectuelle

L'institution rappelle que l'utilisation des ressources informatiques implique le respect des droits de propriété intellectuelle de celle-ci 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 ;
- 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.

Article VI. Respect de la loi informatique et libertés

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 "Informatique et Libertés" modifiée.

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.

Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information.

Ce droit s'exerce auprès du responsable hiérarchique du service ou de l'établissement dont il dépend.

Article VII. Limitation des usages

En cas de non-respect des règles définies dans le présent document, la "personne juridiquement responsable" pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Par "personne juridiquement responsable", il faut entendre toute personne ayant la capacité de représenter l'institution (recteur, directeur académique des services de l'Éducation nationale, personnel d'encadrement et de direction).

Article VIII. Entrée en vigueur des règles d'usage

La date d'entrée en vigueur des règles d'usage est fixée au 14 janvier 2014.

Tout document relatif aux conditions d'utilisation du système d'information doit se conformer aux principes énoncés dans le présent document.

Article IX. Communication électronique

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'utilisation de cette adresse nominative est ensuite de la responsabilité de l'utilisateur.

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.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'institution.

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

(b) Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé⁹ ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place. Dans ce cas, elles seront portées à la connaissance de l'utilisateur du service de messagerie.

⁹ Voir note 4

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

(c) Emission 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^{*10} 1369-1 à 1369-11 du code civil.

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

(e) Fin de fonctions de l'utilisateur

Quand l'utilisateur est déclaré en fin de fonctions, sa boîte aux lettres reste encore opérationnelle pendant un délai de 3 mois au-delà de cette date. Ce délai permettra à l'utilisateur de transférer ou sauvegarder ses messages et d'informer ses correspondants habituels de ses nouvelles coordonnées. Au terme de ce délai de trois mois, la boîte aux lettres sera supprimée.

(f) Stockage et archivage des messages

Chaque utilisateur peut être amené, en raison de contraintes propres à son domaine d'activité, à souhaiter conserver, transférer ou sauvegarder des messages hors de sa boîte aux lettres, notamment parce que ceux-ci pourraient constituer un élément de preuve. Il lui appartient, dans ce cas, de veiller à maintenir un niveau suffisant de protection de la confidentialité des informations contenues dans ces messages.

Section 4.02 Internet

Il est rappelé que l'utilisation d'Internet est soumise à l'ensemble des règles de droit en vigueur. Cette utilisation, tout comme celle des intranets et des extranets, constitue l'un des éléments essentiels d'optimisation du travail par l'amélioration de la mutualisation et de l'accessibilité de l'information au sein et en dehors de l'institution.

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques). Si une utilisation résiduelle privée, telle que définie en section 2.01, est 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.

¹⁰ Issus de la loi n° 2004-575 du 21 juin 2004, modifiés et complétés par l'ordonnance 2005-674 du 16 juin 2005 (ces articles fixent certaines obligations pour la conclusion des contrats en ligne).

(a) Publication sur les sites internet et intranet de l'institution

Toute publication sur les sites internet, intranet ou extranet de l'institution*¹¹ doit être validée par un responsable de site ou responsable de publication.

Aucune publication à caractère privé (pages privées...) sur les ressources du système d'information de l'institution n'est autorisée, sauf disposition dérogatoire établie par un service ou un établissement.

(b) Sécurité

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 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 document 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 formation ou de campagnes de sensibilisation.

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 tels que définis à l'article V.

L'institution 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 (par exemple, des codes malveillants susceptibles d'altérer le bon fonctionnement du système d'information).

Article X. Diffusion des règles d'usage auprès des personnels

L'académie s'engage à communiquer le présent document à ses personnels et à en maintenir un exemplaire consultable sur le site intranet académique IRIA.

¹¹ A partir des ressources informatiques mises à la disposition de l'utilisateur.