

Charte régissant l'usage du système d'information par les personnels du ministère de l'éducation nationale du Vice Rectorat des îles Wallis et Futuna

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 (administration centrale, rectorat, inspection académique), école, ou établissement d'enseignement scolaire.

Le terme d'«utilisateur» recouvre 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.

Il s'agit notamment de :

- *tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'éducation*
- *tout prestataire¹ 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.

¹ Le contrat devra prévoir expressément l'obligation de respect de la charte.

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.

Engagements de l'institution

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

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 déontologie².

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

² Notamment le secret médical dans le domaine de la santé ou s'agissant des situations personnelles connues des personnels sociaux.

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.

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

Section 2.01 Utilisation professionnelle / privée

Les systèmes d'information (notamment messagerie, 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 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 privé dans un espace de données prévu explicitement³ à cet effet ou en mentionnant le caractère privé sur la ressource⁴. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

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

En particulier, la détention, diffusion et exportation d'images à caractère pédophile⁵, ou la diffusion de contenus à caractère raciste ou antisémite⁶ est totalement interdite.

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

Aux seules fins d'assurer la continuité de service (cas de départ notamment), l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition ; ces dispositions peuvent être adaptées lorsque ces ressources présentent un caractère de confidentialité ou de secret avéré.

Si pour des raisons exceptionnelles (absence,...), un utilisateur se trouve dans l'obligation de communiquer ses codes d'accès au système d'information, il doit dès que possible procéder au changement de ces derniers ou en demander la modification à l'administrateur.

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.

³ Par exemple, cet espace pourrait être dénommé "_privé_"

⁴ Par exemple, "_privé_nom_de_l_objet_" : l'objet pouvant être un message, un fichier ou toute autre ressource numérique.

⁵ Article L 323-1 et s. du Code pénal

⁶ Article 24 et 26bis de la Loi du 29 juillet 1881

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 d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'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 ;
- 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 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 précautions:

- de la part de l'institution :
 - o veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie ;
 - o limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- de la part de l'utilisateur :
 - o s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'habilitation explicite ;
 - o ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'institution, ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou l'établissement ;
 - o 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, ou sans autorisation de sa hiérarchie ou de son administrateur du système d'information ;
 - o se conformer (ni les désinstaller, ni les contourner) aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques ;

Section 3.02 Devoirs de signalement et d'information

L'institution doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information. L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, etc. Il signale également à la personne responsable du site toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

Section 3.03 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 opération de maintenance à distance sur les ressources mises à sa disposition est précédée d'une information préalable ;
- 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 est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées. L'institution informe l'utilisateur que le système d'information donne lieu à une surveillance et 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 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 des durées de connexion, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n°78-17 du 6 janvier 1978 modifiée par la loi n°2004-801 du 8 août 2004.

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 identifiées comme telles et relèvent de la vie privée de l'utilisateur.

En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou si elles tombent dans le champ de l'article⁷ 40 alinéa 2 du code de procédure pénale.

⁷ 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. 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 à qui elle a été attribuée.

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 privé⁸ 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, 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 (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques...).

(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 articles⁹ 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) Stockage et archivage des messages

Chaque utilisateur doit organiser et mettre en oeuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve avec les dispositifs mis à sa disposition.

⁸ Par exemple, les messages comportant les termes ("privé") dans l'objet ou sujet du message

⁹ Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne

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.

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, 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.

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

En complément des dispositions légales en vigueur et au regard de la mission éducative de l'institution, la consultation volontaire et répétée de sites à contenus de caractère pornographique depuis les locaux de l'institution est interdite.

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

Toute publication de pages d'information sur les sites internet ou intranet de l'institution¹⁰ 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

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 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.

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 VI.

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 (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'institution, codes malveillants, programmes espions ...).

¹⁰ A partir des ressources informatiques mises à la disposition de l'utilisateur

Article V. Respect de la 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 ;
- 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 ; en particulier la création de fichiers comprenant ce type d'informations et demandes de traitement y afférent sont soumis aux formalités préalables prévues par la loi.

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 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 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.

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

Article VIII. Entrée en vigueur de la charte

Tout document relatif aux conditions d'utilisation du système d'information doit se conformer aux principes de cette charte.

La présente charte a valeur de règlement intérieur pour ce qui concerne l'usage des Systèmes d'information de l'académie.

Elle a fait l'objet d'une présentation devant le CTS de Wallis et Futuna du 23 juin 2015, qui l'a adoptée ; elle entre en vigueur à compter de cette même date.