RÉGION ACADÉMIQUE
PAYS DE LA LOIRE

MINISTÈRE
DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

Académie de Nantes

Charte informatique régissant l'usage du système d'information par les personnels de l'académie de Nantes

CHARTE REGISSANT L'USAGE DU SYSTEME D'INFORMATION PAR LES PERSONNELS DE L'ACADEMIE DE NANTES

SOMMAIRE

Préambule

Par «institution» il faut entendre tout service de l'académie de Nantes y compris les services déconcentrés (rectorat, DSDEN), les écoles (premier degré) et les établissements d'enseignement du second degré.

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

L'informatique nomade (assistants personnels, ordinateurs portables, tablettes, téléphones portables, etc.) est également un des éléments constitutifs du système d'information dès lors qu'il est mis à disposition par l'institution ou qu'il est connecté quand il est personnel.

Le terme d'«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 ;
- 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 implique 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'usage et de sécurité que l'institution et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun. A ce titre l'institution doit la communiquer à l'utilisateur qui en prend connaissance.

Engagements de l'institution

L'institution 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 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 lois en vigueur ainsi que des règles d'éthique professionnelle et de déontologie.

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 ou de son contrat.

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

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 mis à disposition pour des usages professionnels, administratifs et pédagogiques.

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

L'utilisation du système d'information à titre privé doit être résiduelle, tant dans sa fréquence que dans sa durée, et non lucrative. Les conséquences, dont en particulier le surcoût qui en résulte, doivent demeurer négligeables au regard du fonctionnement et du coût global d'exploitation.

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur 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 dénommé explicitement[2] ou en mentionnant le caractère privé sur la ressource[3]. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur qui est responsable de son espace de données à caractère privé. Les espaces de partage fournis par l'institution ne doivent pas servir à cet usage 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.

L'utilisation des systèmes d'information à titre privé doit respecter la législation en vigueur et s'inscrire dans le cadre du respect des obligations et de la déontologie propres aux fonctionnaires rappelés dans la loi n°83-634 du 13 juillet 1983 relative aux droits et obligations des fonctionnaires.

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.

En cas d'absence prolongée (supérieure à 15 jours), l'utilisateur (en particulier les services en contact direct avec le public) devra définir en lien avec son responsable hiérarchique l'utilisation de la fonction de notification d'absence de la messagerie pour indiquer aux interlocuteurs la boite vers laquelle leurs messages devront être réémis, si besoin.

Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'institution.

Section 2.03 Offre de services

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 concerne a minima :

- 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 sauvegarde et la restauration de ses données ;
- un service de téléphonie ;
- un service d'impression.

Dans le cadre d'une compétence partagée, cette offre de services est à mettre en œuvre en partenariat avec la collectivité de rattachement.

---

[2] Par exemple, cet espace pourrait être dénommé "privé".

[3] Par exemple, "privé – nom objet" : l'objet pouvant être un message, un fichier ou toute autre ressource numérique.

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 de l'utilisateur.

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 conférée. 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 ;
- ne pas conserver le NUMEN comme mot de passe ;
- 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 :**

- 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.

✓ **de la part de l'utilisateur :**

- 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 ;
- 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 et/ou ne provenant pas de sites dignes de confiance ;
- se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques ;
- avertir dans les meilleurs délais sa hiérarchie qui en réfère au Responsable de la Sécurité des Systèmes d'Information via la gestion des incidents mise à sa disposition, de tout dysfonctionnement constaté ou de toute anomalie découverte (par exemple une intrusion dans le système d'information ou un accès non autorisé à une ressource sensible ou confidentielle).

Section 3.02 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 ;
- une maintenance à distance est précédée d'une information de l'utilisateur ;
- toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée; le cas échéant supprimée ;
- le système d'information est l'objet d'une surveillance et d'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[4] des accès Internet, de la messagerie et des données échangées.

Préalablement à cette mise en place, l'institution a procédé, auprès du Correspondant Informatique et Libertés (CIL), à une déclaration qui mentionnera notamment la durée de conservation des traces et la durée 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.

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

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, elles relèvent de la vie privée de l'utilisateur.

En revanche l'article[5] 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 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 de la responsabilité de l'utilisateur. La messagerie électronique de l'institution (y compris les messageries intégrées aux outils institutionnels) doit être utilisée pour tout échange professionnel.

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. L'institution déploie des dispositifs « anti-virus » et « anti-spam » qui contribuent à éviter la propagation des virus et bloquent (au mieux des possibilités qu'offre la technique) les messages non sollicités.

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 privé 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, comme l'institution, 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.

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, que l'institution a mis à sa disposition les modalités de sécurité adaptées au niveau de sécurité de l'information traitée.

(d) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent revêtir une forme juridique, sous réserve du respect des conditions fixées par les articles 1125 à 1125-6 du code civil.

[5] 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.

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 œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

(f) Cessation de fonction

En cas de cessation de fonction (mutation, départ à la retraite, etc.), la boite aux lettres nominative professionnelle est maintenue pendant une durée de 6 mois. 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 de service notamment par le transfert des messages reçus au titre de sa fonction précédente.

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.

(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'institution doit être validée par un responsable de site ou un responsable de publication nommément désigné.

Aucune publication de pages d'information à caractère privé 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 des 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 (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'institution, codes malveillants, programmes espions …).

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 liés par convention ou contrat 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 lors de la création de fichiers, auxquelles l'institution elle-même a l'obligation de se conformer.

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.

Sauf mention particulière, ce droit s'exerce auprès du CIL sans préjudice des contestations portées directement à la CNIL.

Article VII. Entrée en vigueur de la charte

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

Adoptée par le comité technique académique du 14 mars 2017, elle entre en vigueur dans toute l'académie et pour tous les personnels à compter de sa publication sur l'intranet « ETNA ».

Article VIII. Dispositions finales

Dans l'hypothèse où des dispositions législatives, réglementaires ou ministérielles viendraient à définir et/ou préciser les conditions d'utilisation des technologies de l'information et de la communication par les personnels, l'académie procéderait aux adaptations éventuellement nécessaires.

Fait à Nantes, le 15 mars 2017

Le recteur de la région académique Pays de la Loire et de l'académie de Nantes, chancelier des universités

William MAROIS