Charte régissant l'usage

du système d'information

de l'académie de Rennes

par les personnels

Sommaire

PRÉAMBULE

Par «institution» s'entend le rectorat de l'académie de Rennes, l'ensemble des services déconcentrés de l'éducation nationale de l'académie de Rennes et les écoles, collèges, lycées.

Par "système d'information" s'entend l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunication, pouvant être mis à disposition par l'institution.

L'informatique nomade (assistants personnels, ordinateurs portables, téléphones portables, etc.) est également un des éléments constitutifs du système d'information.

Par «utilisateur» s'entend tout personnel de l'institution, quel que soit son statut : tout agent titulaire, non titulaire ou bénéficiant d'une convention de stage, ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information.

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

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

➔ Engagements de l'institution

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

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

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

➔ Engagements de l'utilisateur

L'utilisateur est comptable, en toutes circonstances, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et des documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie et des lois en vigueur.

Dans le cas contraire, la responsabilité de l'utilisateur pourra être engagée. Tout abus de l'utilisation des ressources mises à disposition à des fins extra-professionnelles est passible de sanctions. Par ailleurs, le chef de service pourra, sans préjuger des poursuites ou procédures pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Dans tous les cas, l'utilisateur reste soumis au respect des obligations résultant de son statut ou de son contrat.

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.

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

Article II. Conditions d'utilisation du système d'information

Section 1 - Utilisation professionnelle / privée

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

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée qui doivent être qualifiées de personnel. En effet, en l'absence de ce qualificatif, l'information contenue dans l'outil informatique mis à la disposition de l'agent pour l'exécution de son travail, est présumée avoir un caractère professionnel, auquel le recteur ou son représentant pourra avoir accès dans les cas exceptionnels[1] décrits dans les sections 2 et 3.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement[2] à cet effet ou en mentionnant le caractère privé sur la ressource[3]. La sauvegarde régulière des données à caractère privé incombe à l'utilisateur. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace.

Section 2 - Continuité du service : gestion des absences et des départs

L'utilisateur est incité à informer sa hiérarchie des modalités[4] permettant l'accès[5] éventuel aux ressources mises spécifiquement à sa disposition aux seules fins d'assurer la continuité du service.
Aussi, les personnels, notamment ceux exerçant une responsabilité administrative, devront, en cas d'impossibilité prolongée d'accès à leur messagerie, faire en sorte qu'en collaboration avec leur responsable hiérarchique les messages nécessaires au bon fonctionnement du service qui leur parviendraient dans leur boîte nominative ne soient pas perdus. Ils pourront notamment utiliser la fonction de notification d'absence de la messagerie pour indiquer à leurs interlocuteurs la durée prévisible de leur absence et la boîte vers laquelle leurs messages devront être, si besoin, réémis.
Le recteur peut imposer la mise en place de ce message d'absence dans le but exclusif de l'intérêt et de la continuité du service.

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

Section 3- Accès aux données

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

[1] Décès, longue maladie, saisine d'un juge, etc.

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

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

[4] À titre d'exemple, il peut être tenu de communiquer à sa hiérarchie les mots de passe d'accès à son ordinateur et à la messagerie électronique

[5] Identifiants, dispositifs d'accès logique ou physique (carte à puce, clé de sécurité, etc.)

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

Article III. Principes de sécurité

Section 1 - Règles de sécurité applicables

L'institution met en œuvre les mécanismes de protection appropriés sur le système 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 du système d'information mis à sa disposition lui impose de respecter les consignes de sécurité notamment en gardant strictement confidentiel(s) son (ou ses) codes d'accès (sauf cas prévus en section II.2) et en n'utilisant pas les codes d'accès d'un autre utilisateur.

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

➔ de la part de l'institution

- veiller à ce que les ressources confidentielles ou sensibles ne soient accessibles qu'aux personnels habilités ;
- porter à la connaissance de l'utilisateur les éléments susceptibles de lui permettre de sécuriser[6] son utilisation du système d'information.

➔ de la part de l'utilisateur

- ne pas tenter d'accéder à des ressources du système d'information pour lesquelles il n'a pas reçu d'habilitation ;
- ne pas connecter aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'institution ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'institution, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance sans autorisation de sa hiérarchie ;
- se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques ;
- avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute 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 2 - 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 toujours précédée d'une information de l'utilisateur ;

[6] Niveaux de risques encourus : sensibilité de l'application, des données, responsabilité particulière

- toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire sera isolée ; le cas échéant, elle sera supprimée.

Le système d'information donne lieu à une surveillance du bon fonctionnement et à un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

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

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

Article IV. Communications électroniques

Section 1 - Messagerie électronique

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

Un document de conseils d'utilisation de la messagerie électronique professionnelle rappelant les bonnes pratiques en vigueur est disponible sur l'accès webmail, rubrique « Charte ».

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. Elle est à utiliser pour tout échange professionnel.

L'aspect nominatif de l'adresse électronique[7] constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie et ne la rend pas privative.

L'adresse électronique nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.

Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte dans son objet une mention particulière et explicite indiquant son caractère privé[8] ou bien s'il est stocké dans un espace privé de messages ou de donnée.

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

Émission et réception des messages

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

L'utilisation de listes de diffusion institutionnelles relève de la responsabilité de l'institution et de l'utilisateur qui doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés, afin d'éviter notamment l'encombrement inutile de la messagerie ainsi qu'une dégradation du service. L'utilisation de ces listes est réservée à un usage strictement professionnel.

[7] Pour exemple, l'adresse prenom.nom@ac-rennes.fr ou prenom.nom@<nom de domaine institutionnel>.fr

[8] Par exemple, les messages comportant les termes « privé » ou « personnel » dans l'objet ou le sujet du message

Stockage et archivage des messages

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

Préconisations relatives à l'utilisation de la messagerie électronique nominative professionnelle

- L'accès à la messagerie nominative professionnelle de tout poste informatique

Dans le respect des normes nationales, les boîtes de la messagerie nominative du ressort de l'académie de Rennes font partie du domaine « ac-rennes.fr ».
L'accès à la messagerie nominative professionnelle peut s'effectuer de tout poste informatique disposant d'un accès à Internet, y compris du domicile.
Il convient de rappeler que quels que soient le lieu et le mode d'accès à la messagerie nominative professionnelle, les règles prévues par la présente charte s'appliquent intégralement.
Les informations relatives aux différents modes d'accès et à leur paramétrage sont disponibles sur l'accès webmail, rubrique « Mode d'emploi ».
L'institution déploie un dispositif antivirus et un dispositif « antispam » qui contribuent à éviter la propagation des virus et bloquent, au mieux des possibilités qu'offre la technique, les messages non sollicités.
En cas de problème technique, il convient de s'adresser au service d'assistance via le guichet unique (http://assistance.ac-rennes.fr) ou par mél (assistance@ac-rennes.fr) ou encore au 0810 454 454.

La chaîne d'alerte peut également être sollicitée : alerte.ssi@ac-rennes.fr

- La cessation de fonction (mutation, départ à la retraite, etc.)

Dans le cas où l'utilisateur cesse sa fonction, sa boîte aux lettres personnelle est maintenue pendant une durée maximum de 6 mois. Ce délai permet à l'utilisateur d'avertir les correspondants du changement d'interlocuteur et d'assurer la continuité du service notamment par le transfert des messages reçus au titre de sa fonction précédente.

Section 2 - Internet

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

Sur le lieu de travail, Internet est un outil réservé à un usage professionnel avec un usage privé possible dans le respect de la législation en vigueur.

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

L'institution se réserve le droit de filtrer ou d'interdire l'accès à certains sites.

L'accès à Internet n'est autorisé qu'au travers de dispositifs de sécurité mis en place par l'institution qui peut procéder au contrôle des sites visités et des durées d'accès correspondantes.

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 doit être, au préalable, 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.

Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect de la réglementation en vigueur.

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

Article V. Traçabilité

L'institution dispose d'outils de traçabilité de l'utilisation du système d'information pour répondre à l'obligation légale de mettre en place un système de journalisation[9] des accès Internet, de la messagerie et des données échangées.

Article VI. Respect de la propriété intellectuelle

L'institution rappelle que l'utilisation des ressources informatiques et numériques implique le respect des droits de propriété intellectuelle.

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 VII. Respect de la loi « informatique et libertés »

L'utilisateur doit 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 modifiée, dite «Informatique et Libertés» consultable sur le site de la CNIL (www.cnil.fr).

Article VIII. Entrée en vigueur de la charte

La charte a valeur de règlement intérieur pour ce qui concerne l'usage du système d'information. Elle est proposée pour avis aux membres du CTA le 31 mars 2015.

Elle entre en vigueur dans toute l'académie et pour tous les personnels à compter de sa publication sur les sites intranet et internet de l'académie.

Article IX. Dispositions finales

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

Fait à Rennes, le 31 mars 2015.

Le Recteur

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