



Charte régissant l'usage du système d'information par les personnels de l'académie de NANCY-METZ

Sommaire

Préambule	3
Article I. Champ d'application.....	4
Article II. Conditions d'utilisation du système d'information.....	4
Section II.1 – Utilisation professionnelle / privé.....	4
Section II.2 – Continuité de service : gestion des absences et des départs.....	4
Article III. Principes de sécurité.....	5
Section III.1 – Règles de sécurité applicables.....	5
Section III.2 – Devoirs d'information.....	5
Section III.3 – Mesures de contrôle de la sécurité.....	6
Article IV. Communications électroniques.....	6
Section IV.1 – Messagerie électronique.....	6
Section IV.2 – Internet.....	7
Article V. Traçabilité.....	8
Article VI. Respect de la propriété intellectuelle.....	8
Article VII. Respect de la loi « informatique et liberté ».....	8
Article VIII. Entrée en vigueur de la charte.....	9

Préambule

Par "système d'information" s'entend 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 (assistants personnels, ordinateurs portables, téléphones portables,...) est également un des éléments constitutifs du système d'information.

Par «institution», s'entend le rectorat de l'académie de Nancy-Metz et l'ensemble de ses services ou établissements d'enseignement scolaire.

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

Ainsi sont notamment désignés :

- tout agent titulaire, non titulaire ou bénéficiant d'une convention de stage, 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.

La présente charte, qui a fait l'objet d'une consultation du CTPA réuni le 5 juillet 2010, 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 est accompagnée d'un guide juridique qui rappelle les dispositions législatives en vigueur pour son application. Elle peut être complétée par des guides d'utilisation définissant les principales règles pratiques d'usage.

⇒ 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 documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie².

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.

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

² Notamment le secret médical

En tout état de cause, 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 II.1 - Utilisation professionnelle / privée

Le système d'information (messagerie, internet ...) est un outil de travail réservé à un usage professionnel (administratif et pédagogique) mais peut être utilisé à titre privé, de manière résiduelle. 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.

Section II.2 - Continuité de service : gestion des absences et des départs

L'utilisateur peut être tenu d'informer sa hiérarchie des modalités⁵ permettant l'accès⁶ aux ressources mises spécifiquement à sa disposition aux seules fins d'assurer la continuité du service.

Dans ce cas, l'utilisateur procédera, dès que possible, au changement de ses codes d'accès ou en demandera 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.

Article III. Principes de sécurité

Section III.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

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

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

⁵ A titre d'exemple, il peut être amené à communiquer à sa hiérarchie les mots de passe d'accès à son ordinateur et à sa messagerie électronique (boîtes fonctionnelles des secrétariats ...)

⁶ Identifiants, mots de passe, dispositifs d'accès logique ou physique (carte à puce, clés de sécurité ...)

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 du système 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 II.2) ;
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître (sauf cas prévus en section II.2).

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

✓ de la part de l'institution :

- limiter l'accès de l'utilisateur aux seules ressources nécessaires à l'exercice de ses fonctions ;
- 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 (Cf. section II.2) ;

✓ de la part de l'utilisateur :

- s'interdire de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'habilitation explicite ;
- 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 ;
- 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 ;
- se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques ;

Section III.2 - Devoirs d'information

L'institution doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre de sécuriser⁷ son 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 III.3 - 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, elle sera supprimée.

L'institution informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un

⁷ Niveaux de risques encourus : sensibilité de l'application, des données, responsabilité particulière

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. 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 ;
- elles ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité ;
- elles ne tombent pas dans le champ de l'article⁸ 40 alinéa 2 du code de procédure pénale.

Article IV. Communications électroniques

Section IV.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.

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 électronique⁹ constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

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

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 relève de l'utilisation exclusive de l'institution.

Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte dans son objet une mention particulière et explicite indiquant son caractère privé¹⁰ ou bien s'il est stocké dans un espace privé de messages ou de données, comme précisé à la section II.2.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, ces dispositions sont précisées dans un guide technique d'utilisation de la messagerie, porté à la connaissance des utilisateurs.

Sont interdits les messages comportant des contenus à caractère illicite.

L'utilisation de la messagerie professionnelle par les organisations syndicales depuis le système d'information de l'institution, est régie par la charte relative aux usages syndicaux.

Emission et réception des messages

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

⁸ Précisé dans l'annexe Juridique (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 ...)

⁹ Pour exemple, l'adresse prénom.nom@ac-nancy-metz.fr ou prénom.nom@<nom de domaine institutionnel>.fr

¹⁰ Par exemple, les messages comportant les termes (« privé » ou « personnel ») dans l'objet ou sujet du message

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin de limiter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

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 articles¹¹ 1369-1 à 1369-11 du code civil.

L'utilisateur doit, en conséquence, être particulièrement attentif sur la nature des messages électroniques qu'il échange et à ne s'engager par messagerie que s'il est habilité à le faire.

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 constitutifs de son activité professionnelle.

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 par le service ou l'établissement.

Section IV.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.

L'institution met à la disposition de l'utilisateur un accès Internet dans toute la mesure du possible.

Internet est un outil de travail réservé à un usage professionnel et, à titre résiduel, à un usage privé (tel que défini à la section II.2) dans le respect de la législation en vigueur.

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

Publications sur les sites internet et intranet de l'institution

Toute publication de pages d'information sur les sites internet ou intranet de l'institution¹² 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.

Sécurité

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

D'autre part, sous réserve d'en informer les utilisateurs, l'institution peut procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

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 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,...).

¹¹ Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne

¹²A partir des ressources informatiques mises à la disposition de l'utilisateur

Article V. Traçabilité

L'institution se réserve le droit de mettre en place des outils de traçabilité d'utilisation du système d'information. L'institution est dans l'obligation légale de mettre en place un système de journalisation¹³ des accès Internet, de la messagerie et des données échangées.

Par ailleurs, elle procède auprès de la Commission nationale de l'informatique et des libertés (CNIL), 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.

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, 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 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). Le guide juridique précise les termes de la loi.

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.

Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation du système d'information.

Fait à Nancy, le 4 novembre 2010

Le Recteur,



Jean-Jacques POLLET

¹³ Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur ...