ACADÉMIE
DE CRÉTEIL

Liberté
Égalité
Fraternité

Politique de Sécurité des Systèmes d'Information de l'Académie de Créteil

ANNEXE 3

Charte régissant les usages des systèmes d'information et du numérique par les personnels de l'académie de Créteil

Sommaire

I. Contexte....3
II. Objet....3
III. Définitions....4
IV. Champ d'application....5
IV.1. Engagements de l'institution....5
IV.2. Engagements de l'utilisateur....5
V. Conditions d'utilisation des systèmes d'information....6
V.1. Utilisation professionnelle / privée....6
V.2. Télétravail....7
V.3. Continuité de service : gestion des absences et des départs....7
V.4. Assistance et maintenance....8
VI. Principes de sécurité....9
VI.1. Règles de sécurité applicables....9
VI.2. Moyen d'authentification....10
VI.3. Terminaux professionnels / personnels....11
VI.4. Devoirs de signalement et d'information....12
VI.5. Mesures de contrôle de la sécurité....12
VII. Communications électroniques....14
VII.1. Messagerie électronique....14
VII.2. Usage de l'Internet....16
VII.3. Téléchargements....18
VII.4. Traçabilité....18
VIII. Respect de la Propriété intellectuelle....18
IX. Respect de la loi informatique et libertés....19
X. Limitation des usages....19
XI. Entrée en vigueur de la charte....20

I. Contexte

Les informations que nous manipulons tous les jours sont des ressources précieuses et convoitées. Elles sont devenues indispensables à la réalisation de notre mission de service public. De nombreuses composantes pédagogiques, organisationnelles et techniques gravitent et évoluent autour de ces informations. Afin de veiller au bon fonctionnement de cet ensemble, il convient d'en définir un cadre commun d'utilisation.

L'académie est responsable des données qui lui sont confiées, c'est donc à chacun de nous d'en assurer leur protection.

II. Objet

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent, 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 s'engagent à respecter : elle précise les droits et devoirs de chacun.
Un guide juridique annexé à celle-ci rappelle les dispositions législatives et réglementaires en vigueur pour son application.

La charte peut être complétée par des conditions d'utilisation et des guides : ceux-ci définissent les règles spécifiques et pratiques d'usage et ne peuvent pas contrevenir aux principes définis dans cette charte.
Ils correspondent à un ou plusieurs thèmes techniques (usage de la messagerie, usage du poste de travail, guide du filtrage internet, …) et ils peuvent être déclinés par unité fonctionnelle.
Les guides ou les conditions d'utilisation seront élaborés en concertation avec la Direction des Systèmes d'Information et le Responsable Sécurité des Systèmes d'Informations[1].

1 RSSI : Personne chargée de veiller et garantir la sécurité du système d'information de l'institution.

III. Définitions

Système d'information:
Ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'institution et permettant de collecter, regrouper, classifier, stocker, traiter et diffuser de l'information.
L'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portables... est également un des éléments constitutifs du système d'information.

Ressource:
Élément informationnel[2] ou matériel.

Ressource non institutionnelle[3]:
Ressource mise à disposition des utilisateurs par des tiers.

Institution:
Tout service (administration centrale, rectorat, inspection académique) ou établissement d'enseignement relevant de l'Éducation Nationale.

Utilisateur:
Tout personnel habilité ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut.
Sont notamment désignés:
- tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'éducation;
- tout prestataire[4] ayant contracté avec l'institution ou avec une collectivité territoriale ayant compétence partagée avec l'État en matière d'éducation.

2 Pour exemple, une ressource informationnelle peut être un fichier informatique, un document rédigé, etc.
3 Les ressources matérielles personnelles ou les services en ligne proposés par des tiers font parties des ressources non institutionnelles.
4 Le contrat devra prévoir expressément l'obligation de respect de la charte.

IV. 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.
La présente charte s'applique à tous les types d'usages, depuis les locaux des entités ou dans le cadre d'un usage dit « nomade » ou de «télétravail», indépendamment du moyen utilisé pour assurer le traitement ou le stockage de l'information et indépendamment du lieu où l'information est traitée ou stockée, que ce soit au sein d'une entité académique, dans les locaux d'un partenaire institutionnel ou privé, ou à l'extérieur de ceux-ci.

Les usages relevant de l'activité des organisations syndicales sont régis par une circulaire spécifique[5].

IV.1. Engagements de l'institution

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

L'institution met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs, visant à garantir la protection des informations en confidentialité et en intégrité.

L'institution met à disposition de chaque personnel une identité numérique professionnelle donnant accès à ses données de carrière et des données générées dans le cadre de sa pratique professionnelle, ainsi qu'aux systèmes d'information de l'Éducation Nationale.

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

IV.2. 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[6] et du droit de réserve dans ses communications effectuées avec son identité numérique à destination d'acteurs externes à l'institution (messagerie, réseaux sociaux…).
En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

5 Circulaire n° 2012-080 du 20-4-2012

6 Tel qu'il résulte des droits et obligations des fonctionnaires (Loi n°83-634 du 13 juillet 1983) ou notamment le secret médical dans le domaine de la santé.

V. Conditions d'utilisation des systèmes d'information

V.1. Utilisation professionnelle / privée

Les systèmes d'information mis à la disposition de l'utilisateur sont prioritairement à usage professionnel.

Les communications électroniques (messagerie, internet ...) sont des outils de travail ouverts à des usages professionnels, administratifs et pédagogiques et peuvent constituer le support d'une communication privée.

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 explicitement[7] à cet effet ou en mentionnant le caractère privé sur la ressource[8].
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.

Dans le cadre d'une utilisation privée d'une ressource non institutionnelle, celle-ci doit répondre aux exigences de sécurité du système d'information.

L'utilisation des systèmes d'information à titre privé doit respecter la réglementation en vigueur.
En particulier, la détention, diffusion ou exportation d'images à caractère pédophile[9], ou la diffusion de contenu à caractère raciste ou antisémite[10] est totalement interdite.

7 Pour exemple, cet espace pourrait être dénommé "_privé_".
8 Pour exemple, "_privé_nom_de_l_objet_" : l'objet pouvant être un message, un fichier ou toute autre ressource numérique.
9 Article 227-23. du Code pénal
10 Article 24 et 24bis de la Loi du 29 juillet 1881

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

La connexion de matériel professionnel à un réseau externe à l'institution doit faire l'objet d'une vigilance accrue.

V.2. Télétravail

Le télétravail désigne une forme d'organisation du travail dans laquelle un travail, qui aurait pu être exécuté dans les locaux de l'administration, est effectué par un agent hors de ces locaux, de façon régulière et volontaire en utilisant les technologies de l'information et de la communication.
Il se pratique au domicile de l'agent – entendu comme le lieu de sa résidence habituelle – ou, le cas échéant, dans des locaux professionnels distincts de son lieu d'affectation.

Conformément à l'arrêté du 6 avril 2018 portant application dans les services centraux relevant des ministres chargés de l'éducation nationale et de l'enseignement supérieur, les services déconcentrés et les établissements relevant du ministre de l'éducation nationale du décret n° 2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature, le télétravailleur bénéficie des mêmes droits et est soumis aux mêmes obligations que les agents travaillant sur site, tels que décrits dans la présente charte.

Il s'engage également à respecter la confidentialité des informations détenues ou recueillies dans le cadre de leur activité et à veiller à ce qu'elles ne soient pas accessibles à des tiers.

Les conditions et modalités d'organisation du télétravail sont définies entre le responsable de service ou de division et l'agent dans une convention individuelle de télétravail.

V.3. Continuité de service : gestion des absences et des départs

En cas d'absence et aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie, en en informant le RSSI, des modalités[11] permettant l'accès aux ressources mises spécifiquement à sa disposition[12].

En cas d'absence de l'agent, l'institution, par le RSSI, peut être amenée à accéder à ses données professionnelles pour assurer la continuité de service. L'institution doit en informer au préalable l'agent.

11 À titre d'exemple, en cas d'absence ou de départ, si nécessaire, il devra communiquer à sa hiérarchie les mots de passe d'accès au système d'information.

12 Ces dispositions peuvent être adaptées en fonction de la spécificité des activités exercées, notamment lorsque des données présentent un caractère de confidentialité ou de secret avéré.

En cas d'absence non planifiée et pour des raisons exceptionnelles, si un utilisateur se trouve dans la situation de communiquer ses codes d'accès[13] au système d'information, il doit procéder, dès que possible, au changement de ces derniers ou en demander la modification à l'administrateur.

L'institution ne peut, sans violer le droit au respect de la vie privée, consulter les messages électroniques et les fichiers portant explicitement une mention du caractère privé par l'indication par exemple de « personnel », « privé » ou étant connus comme personnels, sauf risque ou évènement particulier[14].

Seuls le RSSI ou son adjoint peuvent délivrer les accès aux données de l'agent absent.

L'institution recommande aux utilisateurs d'utiliser les espaces partagés qu'elle leur met à disposition (partages réseaux, outils de synchronisation et de partage de données, Environnements Numériques de Travail…) pour y stocker ses données professionnelles, afin de faciliter la transmission des informations en cas d'arrivée et de départ.

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

V.4. Assistance et maintenance

En cas de question relative au fonctionnement du système d'information, l'utilisateur consultera la documentation mise à sa disposition.

En cas de problème relatif au fonctionnement du système d'information ou de demande spécifique, l'utilisateur se rapprochera de son service d'assistance technique.

Pour effectuer la maintenance corrective, évolutive ou à des fins de restauration, dans la mesure du possible, l'institution se réserve la possibilité de réaliser des interventions sur les ressources mises à la disposition de l'utilisateur.

13 Identifiants, mots de passe, dispositifs d'accès logique ou physique (carte à puce, clés de sécurité …)
14 Cass. soc. 17-5-2005 pourvoi 03-40017 : « sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé. »

VI. Principes de sécurité

VI.1. 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 et moyens d'accès (cartes magnétiques, clés OTP ou ODA, etc.) 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 lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès comme la modification cyclique et la complexité des mots de passe,
- de se connecter et de s'authentifier sur le réseau de l'institution en utilisant uniquement les terminaux mis à disposition par l'institution (sauf cas prévus dans la présente charte) et les moyens ou méthodes sécurisés mis en place à cet effet par l'institution (authentification sur le réseau local, accès par un client « VPN » spécifique ou site extranet sécurisé),
- de garder strictement confidentiels ses codes d'accès et ne pas les dévoiler à un tiers (sauf cas prévus dans la présente charte),
- 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 :

<u>De la part de l'institution</u>

- 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,
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

<u>De la part de l'utilisateur</u>

- 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 connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'institution,
- ne pas créer, copie, installer, télécharger ou utiliser sur le matériel de l'institution, des ressources dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance sans l'autorisation du RSSI ou de son adjoint,
- se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques.

VI.2. Moyen d'authentification

L'utilisateur est informé que les moyens d'authentification permettant l'accès au système d'information constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive.
Cette mesure ne confère pas aux ressources protégées un caractère privé.

Les droits d'accès et les habilitations accordés à l'utilisateur sont définis en fonction de sa mission et de son niveau d'exercice.

La sécurité des systèmes d'information mis à la disposition de l'utilisateur lui impose de respecter les consignes et les règles de sécurité relatives à la gestion de l'authentification et à la gestion des accès.

Il doit notamment :

- garder strictement confidentiels ses moyens d'authentification et ne pas les dévoiler à un tiers,
- ne pas utiliser les noms et moyens d'authentification d'un autre utilisateur, ni chercher à les connaître,
- veiller à ne pas garder un accès ouvert à une ressource sans surveillance.

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son ou ses moyens d'authentification, il devra procéder, dès que possible, au changement de ce dernier ou en demander la modification à l'administrateur.
Le bénéficiaire de la communication du moyen d'authentification veillera à s'assurer de garder une trace de cette communication.
Il ne peut le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle à l'origine de la communication.

VI.3. Terminaux professionnels / personnels

L'agent est doté d'un terminal par l'académie ou la collectivité territoriale

La connexion de terminaux personnels aux réseaux locaux de l'institution ou à distance n'est pas autorisée lorsque l'agent est doté d'un terminal par l'académie ou la collectivité territoriale.
L'usage de terminaux professionnels est dans ce cadre imposé, notamment en situation de télétravail.

L'agent n'est pas doté d'un terminal par l'académie ou la collectivité territoriale

En cas d'absence de dotation de matériels dédiés aux usages professionnels par l'académie ou la collectivité territoriale, les agents peuvent être amenés à connecter leurs terminaux personnels (BYOD)[15] aux réseaux locaux.

Cas d'usages non autorisés

- la connexion aux réseaux administratifs des établissements du second degré,
- la connexion aux réseaux filaires des services académiques,
- la connexion au réseau RACINE-API sans l'accord explicite du RSSI.

Cas d'usages autorisés
Après accord de l'académie ou de la collectivité territoriale, peuvent être admis:

- la connexion aux réseaux et systèmes pédagogiques des écoles du premier degré, des établissements du second degré et des CIO,
- la connexion à des réseaux filaires ou sans fil de type «invités», permettant uniquement un accès filtré vers internet et ne permettant pas d'accéder aux ressources du réseau local,
- l'utilisation d'un terminal personnel dans un cadre de travail à distance ou au domicile (notamment pour l'activité professionnelle des enseignants en cas de confinement)

Ces terminaux personnels doivent en complément respecter les recommandations suivantes :

- disposer d'un système d'exploitation à jour: dans cette optique, l'utilisateur doit seulement s'assurer que les mises à jour automatiques sont bien activées sur son terminal, et s'assurer régulièrement de leur bonne installation,
- disposer d'un antivirus à jour ou d'un équivalent,
- disposer des dernières mises à jour des autres applications mises à disposition par l'institution ou la collectivité territoriale, lorsqu'elles le sont également pour une installation sur un terminal personnel,

15 Terminaux désignés sous les acronymes BYOD (Bring your Own Device) ou AVEC (Apportez Votre Équipement personnel de Communication)

- lors de leur utilisation en liaison avec un matériel ou un réseau pédagogique, être si possible utilisés avec un compte ne disposant pas de droits d'administration sur le terminal.

VI.4. 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, une exfiltration de données, etc.

Il signale également toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation en déclarant un incident de sécurité au RSSI ou auprès de la collectivité territoriale en charge de son établissement.

VI.5. 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 maintenance à distance est précédée d'une information de l'utilisateur,
- que toute opération bloquante pour le système ou générant une difficulté technique sera interrompue et bloquée. Le cas échéant, les fichiers transmis lors de ces opérations pourront être supprimés.

L'institution informe l'utilisateur que le système d'information peut donner 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 est dans l'obligation légale de mettre en place un système de journalisation[16] des accès Internet, de la messagerie et des données échangées.

Préalablement à cette mise en place, l'institution procédera, auprès du délégué à la protection des données de l'académie (DPD), 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 et de la loi n° 2018-493 du 20 juin 2018[17].

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

Les personnels en charge de ces 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 qu'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'article[18] 40 alinéa 2 du code de procédure pénale.

VII. Communications électroniques

VII.1. Messagerie électronique

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

Les communications professionnelles par message électronique se feront uniquement via les messageries et les adresses électroniques professionnelles nominatives, fonctionnelles ou organisationnelles mises à disposition par l'institution.

Pour préserver la sécurité et le bon fonctionnement du système d'information, des filtres et des limitations techniques sur l'utilisation de la messagerie peuvent être mises en place.

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 cette adresse électronique ne retire en rien le caractère professionnel de celle-ci.
Elle peut cependant constituer le support d'une communication privée telle que définie dans la présente charte et dans le respect de la législation en vigueur.

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

17 La loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi Informatique et Libertés du 6 janvier 1978 afin d'exercer certaines des « marges de manœuvre nationales » autorisées par le Règlement général sur la protection des données (RGPD) et de transposer en droit français la Directive « police-justice ». Elle a également modifié certaines dispositions de la loi Informatique et Libertés pour les rapprocher de la lettre du RGPD.

18 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 ...)

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 adresses ne peuvent être utilisées sans autorisation explicite.

Contenu des messages électroniques

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.

Tout message est réputé professionnel, sauf s'il comporte une mention particulière et explicite indiquant son caractère privé[19] ou s'il est stocké dans un espace privé de données.

L'utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques.

Sont interdits les messages comportant des contenus à caractère illicite quelles qu'en soient leur 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.

L'utilisation de la messagerie professionnelle par les organisations syndicales depuis les systèmes d'informations de l'institution est régie par la charte relative aux usages syndicaux si elle existe telle que définie dans la circulaire n° 2012-080 du 20/04/2012.

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.

Statut et valeur juridique des messages

Les messages échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles[20] 1369-1 à 1369-11 du code civil.

19 Par exemple, les messages comportant les termes «privés» ou «perso» dans l'objet ou sujet du message.
20 Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne.

L'utilisateur est informé qu'un message électronique peut constituer une preuve susceptible d'engager la responsabilité de l'institution ainsi que la sienne.
L'utilisateur doit, en conséquence, être vigilant quant à la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

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, avec les moyens mis à sa disposition.

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 établis par le service ou l'établissement.

Règles du bon usage de la messagerie

Afin de garantir le bon acheminement, les utilisateurs doivent respecter les règles d'usage de la messagerie académique suivantes :

- faire un usage raisonné de la messagerie et ne pas surcharger les boîtes de messagerie internes ou externes,
- ne pas diffuser de messages de type canulars, chaînes, escroquerie par hameçonnage (phishing), jeux, etc.
- ne pas utiliser d'adresse électronique professionnelle dans un contexte non professionnel. En particulier, ne pas l'utiliser sur des sites internet (groupes de discussion (chats), commerce, forums, blogs, etc…), sans rapport avec l'activité professionnelle,
- ne pas rediriger manuellement ou automatiquement les messages professionnels reçus sur la messagerie académique vers une messagerie personnelle, conformément à l'interdiction posée par le ministère. En cas de redirection le non acheminement des messages professionnels n'est pas de la responsabilité de l'académie,
- ne pas utiliser d'adresses de messageries personnelles dans un contexte professionnel,
- pour des raisons de sécurité et de confidentialité, l'utilisation d'une boîte à lettres professionnelle à titre privé n'est pas recommandée,
- s'assurer, à chaque envoi de données, en particulier sensibles, que tous les destinataires sont appropriés ;
- ne pas ouvrir les messages douteux et les pièces jointes suspectes, ne pas répondre aux émetteurs, et ne pas cliquer sur les liens présents dans ces messages,
- prévenir l'assistance informatique en cas de doute, et même après l'ouverture d'un message ou avoir cliqué sur un lien qui s'avère a posteriori douteux.

VII.2. Usage de l'Internet

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

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.

L'utilisation de sites internet institutionnels pour consulter, traiter, ou stocker des informations professionnelles doit être privilégiée.
A contrario, certains critères de sécurité doivent être vérifiés et le cas échéant soumis à validation du RSSI ou de son adjoint (localisation des données, types de données traitées, transferts de données, chiffrement…).

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques): il peut constituer le support d'une communication privée telle que définie dans la présente charte et 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, il est rappelé que la consultation volontaire de sites à contenus de caractère pornographique depuis les locaux de l'institution ou des terminaux mis à disposition par 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'institution[21] doit être validée par un responsable de site ou 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.

Sécurité

L'accès Internet 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.

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

L'Institution se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder, dans un cadre légal, au contrôle à priori ou à posteriori des sites visités et des durées d'accès correspondantes.

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.

VII.3. 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 dans la présente charte.

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, etc.).

VII.4. Traçabilité

L'institution est dans l'obligation légale de mettre en place un système de journalisation[22] des accès Internet, de la messagerie et des données échangées.

L'institution se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes d'information.

VIII. 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.

Les développements informatiques faits par un agent de l'État dans le cours de l'exercice de ses fonctions, s'inscrivant dans le domaine des activités du service, ou grâce à la connaissance ou l'utilisation des techniques ou de moyens spécifiques au service, ou de données procurées par celui-ci, sont susceptibles d'appartenir à l'État.

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

IX. 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 par la loi n° 2004-801 du 6 août 2004.

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.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « Informatique et Libertés », comme l'inscription au registre des traitements de l'établissement ou de l'académie.

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer son supérieur hiérarchique, responsable des traitements de données à caractère personnelles.

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 délégué académique à la protection des données de l'académie (DPD).

X. 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 », on entend : toute personne ayant la capacité de représenter l'institution (recteur, directeur académique, chef d'établissement, directeur d'établissement...).

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles, est passible de sanctions.

Sont susceptibles d'être regardés comme abusifs tous comportements :

- visant à induire en erreur ou à outrepasser les mesures de sécurité mises en œuvre pour assurer le bon fonctionnement des services,
- ayant entraîné une consommation manifestement excessive, au regard des missions confiées à l'utilisateur, sur un ou plusieurs abonnements ou autres ressources mises à disposition,
- ayant entraîné la diffusion volontaire d'informations à des destinataires n'ayant aucun besoin légitime de connaître leur contenu,
- ayant entraîné la diffusion de données comportant des contenus à caractère illicite (notamment ceux attentatoires à vie privée d'autrui, diffamatoires ou relevant de l'injure, attentatoires à la liberté d'expression, de nature à provoquer des mineurs à commettre des actes illicites ou dangereux, faisant l'apologie du terrorisme, etc.),
- ayant entraîné le téléchargement, l'installation, ou l'utilisation sur le matériel de l'institution, de logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou dépourvus d'autorisation de sécurité délivrée la par l'académie.

XI. Entrée en vigueur de la charte

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

Elle est annexée au règlement intérieur des services déconcentrés de l'Éducation Nationale dans l'académie de Créteil.

Elle fait également l'objet d'une communication devant le conseil d'administration des établissements publics locaux d'enseignement de l'académie de Créteil.

La présente charte entre en vigueur dès son approbation en Comité Social d'Administration.

Toutes les règles relatives à l'utilisation des systèmes d'information entrant en conflit avec les présentes règles sont annulées et remplacées par celles-ci.