académie Créteil

RÉGION ACADÉMIQUE
ÎLE-DE-FRANCE

MINISTÈRE
DE L'ÉDUCATION NATIONALE
ET DE LA JEUNESSE

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Charte régissant l'usage des technologies de l'information et de communication par les personnels de l'académie de Créteil

Document présenté en Comité Technique Académique le 4 octobre 2019

Table des matières

1. 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 la protection.

2. OBJET

Le bon fonctionnement du système d'information implique le respect des règles visant à assurer la sécurité, la performance des traitements, la préservation des données et le respect des dispositions légales et réglementaires qui s'imposent.

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 les devoir de chacun.

Elle a aussi pour vocation de sensibiliser les utilisateurs aux exigences de sécurité et d'attirer leur attention sur certains comportements pouvant porter atteinte à l'intérêt collectif du service public d'éducation.

La charte est accompagnée d'un guide juridique qui rappelle les dispositions législatives et règlementaires en vigueur pour son application. Elle 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].

3. DEFINITION

Dans la présente charte, les termes suivants ont le sens qui leur est donné ci-dessous.

- **Institution** : toute structure académique (rectorat, direction des services départementaux, circonscription), centre d'information et d'orientation, écoles ou établissement public local d'enseignement
- **Ressource** : élément informationnel[2] ou matériel ;
- **Système d'information** : ensemble des ressources permettant de collecter, regrouper, classifier, stocker, traiter et diffuser de l'information quel que soit le support (numérique, papier, …) ;
- **Utilisateur** : toute personne, quel que soit son statut, ayant accès, dans l'exercice de son activité professionnelle, aux ressources du système d'information de l'académie de Créteil.
- **Ressource non institutionnelle[3]** : ressource mise à disposition des utilisateurs par des tiers.

[1] RSSI : Personne chargée de veiller et garantir la sécurité du système d'information de l'institution.
[2] Pour exemple, une ressource informationnelle peut être un fichier informatique, un document rédigé, …
[3] Les ressources matérielles personnelles ou les services en ligne proposés par des tiers font parties des ressources non institutionnelles.

4. CHAMP D'APPLICATION

La présente charte s'applique à l'institution ainsi qu'à l'ensemble des utilisateurs de son système d'information.

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[4] ayant contracté avec l'institution ou avec une collectivité territoriale ayant compétence partagée avec l'académie de Créteil en matière d'éducation.

5. ENGAGEMENTS DE L'INSTITUTION

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

L'institution s'engage à 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.

L'institution est tenue de respecter la vie privée de chacun.

6. ENGAGEMENT 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 ressources auxquelles il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie[5].

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

7. CONDITIONS D'UTILISATION DU SYSTEME D'INFORMATION

7.1. Professionnelle / privée

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

L'utilisation à des fins privées doit être non lucrative et raisonnable, tant dans la fréquence que dans la durée. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service. En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des systèmes d'information doit demeurer négligeable au regard du coût global d'exploitation.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées[6] 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 à cet effet.

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

[4] Le contrat devra prévoir expressément l'obligation de respect de la charte académique d'utilisation du système d'information.
[5] Tel qu'il résulte des droits et obligations des fonctionnaires (Loi n°83-634 du 13 juillet 1983).
[6] Une dénomination "Personnel & Privé" ne pourra pas porter à équivoque.

L'utilisation des systèmes d'information à titre privé doit respecter la règlementation en vigueur[7]. En particulier, la détention, diffusion ou exportation d'images à caractère pédophile[8], ou la diffusion de contenu à caractère raciste ou antisémite[9] est totalement interdite.

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 est interdite.

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.

7.2. Continuité de service : gestion des absences et des départs

Pour assurer la continuité de service, l'utilisateur doit informer sa hiérarchie des modalités permettant l'accès aux systèmes d'information dont il dispose[10].

Lors de son départ définitif du service ou de l'établissement, il appartient à l'utilisateur de veiller à laisser les ressources utilisées dans un état impersonnel et de détruire ses données à caractère privé. La responsabilité de l'institution ne pourra être engagée quant à la conservation et la confidentialité de ces données.

Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'institution. Toutes les ressources mises à disposition de l'utilisateur telle que l'adresse de messagerie ne seront plus fonctionnelles ou accessibles par l'utilisateur à l'échéance du délai défini dans ces mesures de conservation.

7.3. 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.

8. PRINCIPE DE SECURITE.

8.1. 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 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 des missions qui lui sont conférées. 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 ;

[7] Voir le guide juridique de l'utilisateur du système d'information de l'académie de Créteil.
[8] Article 227-23. du Code pénal
[9] Article 24 et 24bis de la Loi du 29 juillet 1881
[10] Cette disposition ne concerne pas les personnels de santé qui sont tenus au secret professionnel (Article L4314-3 du code de la santé publique)

- De garder strictement confidentiels ses codes d'accès et ne pas les dévoiler à un tiers ;
- De respecter la gestion des accès, en particulier les codes d'accès d'un autre utilisateur, ni chercher à les connaitre.

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

De la part de l'institution

- Veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité de service mises en place par la hiérarchie (cf. paragraphe 7.2)
- Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

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 relier, créer, installer, copier, télécharger ou utiliser sur le système d'information des ressources autres que celles mises à disposition 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, ou sans autorisation de sa hiérarchie ;
- se conformer aux dispositifs mis en place par l'institution pour lutter contre les menaces et les attaques sur le système d'information ;

D'une manière générale, une autorisation exceptionnelle, accordée à un utilisateur et sortant du cadre de sa mission habituelle, n'est opposable que si elle est formelle et consignée.

8.2. 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 :

- Choisir et utiliser des mots de passe robustes, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne[11]
- garder strictement confidentiel(s) son (ou ses) moyen(s) d'authentification et ne pas le(s) 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.

[11] L'ANSSI (Agence nationale de la sécurité des systèmes d'information) met à disposition une fiche pratique « Sécurité des mots de passe ».

8.3. Devoir de signalement et d'information

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte lié au système d'information. Il signale également toute possibilité d'accès à une ressource du système d'information qui ne correspond pas à son habilitation. Ces informations doivent être portées à la connaissance de la personne responsable de la ressource concernée ou au RSSI de l'institution.

8.4. 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 (transfert de courriel trop volumineux ou transportant un programme potentiellement malveillant, téléchargement ou téléversement de fichiers volumineux etc..) 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 donne lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité règlementaire 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[12] des accès Internet, de la messagerie et des données échangées.

Préalablement à cette mise en place, l'institution procèdera, auprès du délégué à la protection des données de l'académie, 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[13].

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 , sauf si elles mettent en cause le bon fonctionnement technique des application ou leur sécurité , ou si elles tombent dans le champ de l'article 40 alinéa 2[14]du code de procédure pénale.

9. COMMUNICATION ELECTRONIQUE

9.1. 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.

[12] Conservation des informations techniques de connexion telle que l'heure d'accès, l'adresse IP de l'utilisateur.
[13] 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.
[14] 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.

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.

9.1.1. Adresses électroniques

L'institution s'engage à mettre à la disposition de l'utilisateur une adresse de messagerie électronique 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 au paragraphe 7.1 dans le respect de la législation en vigueur. 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, 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.

9.1.2. Contenu des messages électroniques

Tout message est réputé professionnel, sauf s'il comporte une mention particulière et explicite indiquant son caractère privé[15] 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 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 d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par injure non publique, protection du droit d'auteur, protection des marques…).

9.1.3. Emission 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 électronique ainsi qu'une dégradation du service.

9.1.4. 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 1369-1 à 1369-11[16] du code civil.

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 sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

9.1.5. 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.

[15] Par exemple, les messages comportant les termes « privés » dans l'objet ou sujet du message.

[16] Issus de l'ordonnance n°2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique.

9.2. Usage de l'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). Il peut constituer le support d'une communication privée telle que définie en section 7.1 dans le respect de la législation en vigueur.

9.2.1. Publication sur des sites internet et intranet de l'institution

Toute communication des pages sur les sites internet ou intranet de l'institution doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication de pages d'information à caractère privé sur des ressources du système d'information de l'institution n'est autorisée, sauf disposition particulière précisée dans le guide d'utilisation établi par le service ou l'établissement.

9.2.2. Sécurité

L'accès à internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution. En complément des dispositions légales en vigueur, l'institution se réserve le droit de limiter, sélectionner ou restreindre l'accès à certains contenus ou services internet.

9.3. Téléchargement

Tout téléchargement de fichiers, notamment de sons ou d'images sur Internet, doit s'effectuer dans le respect des droits de la propriété intellectuelle tel que défini à l'article 5.

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, codes malveillants, programmes espions…).

10. RESPECT DE LA PROPRIETE 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 :

- veiller à respecter les conditions des licences souscrites ou s'assurer de respecter les dispositions légales liées à l'exception pédagogique ;
- 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.

11. RESPECT DE LA LOI INFORMATIQUE ET LIBERTE ET DU RGPD[17]

Conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi qu'aux disposition de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'Information.

Ce droit s'exerce auprès du responsable hiérarchique du service ou de l'établissement dont il dépend.

[17] Règlement général sur la protection des données.

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à cette loi.

Les données à caractère personnel sont des informations qui permettent - **sous quelque forme que ce soit** - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

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 » et le RGPD.

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement les services compétents qui prendront les mesures nécessaires au respect des dispositions légales.

12. LIMITATION DES USAGES

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les différents guides d'utilisation, 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 des services de l'éducation nationale, chef 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.

13. ENTREE EN VIGUEUR DE LA CHARTE

La présente charte entre en vigueur dès sa présentation en Comité Technique Académique.

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.