RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

les Crous

CHARTE RELATIVE AUX USAGES DU NUMERIQUE

Préambule

Le système d'information et plus généralement le numérique du Cnous sont des outils de travail réservés aux usages professionnels pouvant, à titre résiduel et suivant les dispositions prévues à cette charte, être le support d'une utilisation relevant de la vie privée de l'utilisateur. La pluralité des lieux de travail (et notamment l'accès de l'extérieur de l'établissement aux ressources du système d'information) n'altère en rien le caractère professionnel 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 l'utilisation et la conservation des données.

La présente charte définit les règles d'usage et de sécurité que l'établissement et l'utilisateur s'engagent à respecter ; elle précise les droits et devoirs de chacun.

Elle n'a pas pour objet et objectif de couvrir de façon exhaustive tous les cas de figure pouvant se présenter dans le cadre de l'utilisation des moyens informatiques et de communication électronique mis à la disposition par l'établissement. C'est dans l'esprit des règles présentées dans ce document que chacun devra se conformer dans des situations non envisagées.

La présente charte est susceptible d'évoluer en fonction du contexte règlementaire, légal ou technologique.

Les règles d'usage et de sécurité s'appliquent à l'établissement ainsi qu'à l'ensemble des utilisateurs. La charte peut être complétée par des guides d'utilisation définissant les principales règles d'usage.

Article I. Champ d'application

Par « système d'information » s'entend l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications composant le numérique des Crous et pouvant être mis à disposition par l'établissement.

Les outils de la mobilité (tels que les ordinateurs portables, les téléphones portables …) mis à disposition par l'établissement sont également des éléments constitutifs du système d'information.

Par « établissement », s'entend le Cnous.

Par « chef d'établissement » , s'entend la présidente ou le président du Cnous.

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

Ainsi sont notamment désignés :

- Tout utilisateur, agent titulaire et non titulaire ou bénéficiant d'une convention de stage, concourant à l'exécution des missions de l'établissement ;
- Tout prestataire[1] ayant contracté avec l'établissement ;
- Toute personne qui serait amenée à utiliser toute ou partie du système d'information.

Article II. Portée et opposabilité

La présente charte est annexée au règlement intérieur de l'établissement.

L'établissement est tenu de la porter à la connaissance de l'utilisateur et en conséquence, l'utilisateur doit attester la prise de connaissance

Section 2.01 RESPONSABILITES ET ENGAGEMENTS DE L'ETABLISSEMENT

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

L'établissement met en œuvre les mesures pour assurer la sécurité du système d'information et la protection des utilisateurs. L'établissement facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont à usage professionnel mais l'établissement est tenu de respecter la vie privée de chacun.

Section 2.02 RESPONSABILITES ET ENGAGEMENT DE L'UTILISATEUR

L'utilisateur est responsable, en toutes circonstances, de l'usage qu'il fait du système d'information auquel il a accès. L'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat. 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. Le non-respect de ses obligations ou tout abus dans l'utilisation des ressources mises à sa disposition engagent la responsabilité de l'utilisateur et peut donner lieu à des procédures disciplinaires et/ou des poursuites pénales. Sans préjuger des poursuites ou procédures engagées, l'établissement peut limiter, par mesure conservatoire, l'usage du système d'information pour l'utilisateur concerné.

Article III. Principes de sécurité

Section 3.01 REGLES APPLICABLES

L'établissement met en œuvre les mécanismes de protection appropriés sur le système d'information mis à la disposition des utilisateurs.

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

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité 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 ;
- Garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers sauf cas prévus pour la continuité de service, en section 4.02 ;
- 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 obligations :

a) De la part de l'établissement

- 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 4.02) ;
- Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

b) 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 connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'établissement, 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 les matériels de l'établissement, 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'établissement pour lutter contre les virus et les attaques par programmes informatiques.

Section 3.02 DEVOIR D'INFORMATION

L'établissement doit porter à la connaissance de l'utilisateur, dès sa prise de fonction, tout élément susceptible de lui permettre de sécuriser son utilisation du système d'information.

L'utilisateur doit signaler dans les meilleurs délais au Responsable de la Sécurité de Système d'information (RSSI – rssi@cnous.fr) et selon la nature de l'incident, au Délégué à la Protection des Données (DPO – dpo@cnous.fr) de tout dysfonctionnement constaté ou de toute anomalie découverte (un défaut de sécurité, une intrusion dans le système d'information, …).

Section 3.03 MESURE DE CONTROLE DE LA SECURITE

L'utilisateur est informé que :

- Pour effectuer la maintenance corrective, curative ou évolutive, l'établissement se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- 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'établissement 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'utilisateur est informé préalablement à tout contrôle ou à toute intervention sur une ressource mise à sa disposition (ordinateur, téléphone, …).

Les personnels chargés des opérations de contrôle du système d'information sont soumis à des règles de confidentialité renforcées.

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'article 40 alinéa 1 du code de procédure pénale.

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

Section 4.01 UTILISATION PROFESSIONNELLE / PRIVEE

Toute ressource numérique confiée à l'utilisateur est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Les ressources numériques (ordinateur, téléphone, données, mails, …) et les outils de communications électroniques (messagerie, internet …) sont des outils de travail réservés à un usage professionnel et peuvent également constituer, à titre résiduel, le support d'une utilisation ou communication privée. Il convient, dans ce cas, de préfixer l'objet du message par le texte suivant : "[Privé]".

- L'utilisation résiduelle à titre privé des ressources et outils mis à disposition de l'utilisateur doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. L'utilisation à titre privé (en temps et en coût généré) doit demeurer négligeable par rapport aux usages professionnels ;
- 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.

Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données ou en mentionnant le caractère privé sur la ressource (Se conformer aux consignes locales de la direction du numérique).

Le nom de cet espace doit contenir la chaîne de caractère [privé] pour que soit appliquéle principe du secret des correspondances.

Section 4.02 CONTINUITE DU SERVICE

L'établissement organise la continuité de service notamment pour prendre en compte les absences ou indisponibilité de l'utilisateur.

En cas de nécessité avérée et sur décision du chef d'établissement notifiée à l'utilisateur, il peut être exigé que l'utilisateur fournisse les modalités permettant l'accès à toute ou partie des ressources mises à sa disposition (code d'accès). En cas de force majeure, l'établissement se réserve le droit de forcer l'accès aux ressources mises à disposition avec information préalable de l'utilisateur.

Section 4.03 GESTION DES DEPARTS

Lors de son départ définitif de l'établissement, l'utilisateur remet l'ensemble des ressources numériques qui ont été mises à sa disposition suivant les modalités définies par l'établissement.

L'utilisateur ne peut détruire toute ou partie de ses données professionnelles sans avis de sa hiérarchie. Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'établissement. Il lui appartient de détruire son espace ou ses données à caractère privé, la responsabilité de l'établissement ne peut être engagée quant à la conservation de ces données après son départ.

Article V. Communications électroniques

Section 5.01 MESSAGERIE ELECTRONIQUE ET TRAVAIL COLLABORATIF

L'utilisation de la messagerie électronique professionnelle constitue l'un des éléments d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'établissement. Les règles définies ci-dessous s'appliquent également aux outils de travail collaboratif généralement liées à la messagerie de l'établissement.

a) Adresses électroniques

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

L'adresse électronique[2] 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'établissement.

Un message ne peut être anonyme. A minima, tout message envoyé d'une adresse non nominative (exemple : adresse fonctionnelle) doit être signé au nom du rédacteur.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles relève de la responsabilité exclusive de l'établissement.

b) 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[3] ou bien s'il est stocké dans un espace privé de messages ou de données.

c) 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 de limiter les diffusions inutiles de messages en masse.

d) Statut et valeur juridique des messages

Tout message électronique échangé avec des tiers peut engager la responsabilité, au plan juridique, de l'établissement. L'utilisateur doit, en conséquence, être particulièrement attentif sur la nature des messages électroniques qu'il échange et àne s'engager par messagerie que s'il est habilité à le faire.

e) Bon usage de la messagerie

L'utilisateur s'engage à respecter les règles suivantes :

- Ne pas utiliser son 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 qu'il reçoit sur sa messagerie professionnelle vers une messagerie personnelle ;
- Ne pas utiliser une adresse de messagerie personnelle dans son contexte professionnel ;
- Ne pas utiliser la messagerie pour l'envoi de fichiers volumineux ;
- Ne pas utiliser la messagerie pour l'envoi de

[2] L'adresse est de la forme prenom.nom@crous-xxxx.fr ou prenom.nom@cnous.fr

[3] Voir article IV section 4.01

fichiers comprenant des données personnelles ou sensibles (se référer au délégué à la protection des données en cas de doute) .

- **Devoir de vigilance**

L'établissement met en œuvre les mécanismes pour protéger la messagerie des principaux risques liés notamment à des usurpations d'identité et messages douteux. Ces protections ne peuvent garantir une totale efficience notamment contre les campagnes d'hameçonnage (phishing).

L'utilisateur a un devoir de vigilance et doit prévenir l'assistance informatique en cas de doute ou après avoir ouvert un message ou cliqué sur un lien qui s'avère a posteriori douteux.

f) Stockage et archivage des messages

L'utilisateur doit 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.

Section 5.02 AGENDA ELECTRONIQUE

L'utilisation et la mise à jour de l'agenda électronique constituent une obligation de service pour tout utilisateur du Cnous. Toute réunion, déplacement ou événement impliquant une disponibilité réduite pendant les horaires de travail doit figurer sur l'agenda. Il est conseillé d'y faire également figurer ses périodes de congés et de télétravail.

L'agenda de tout utilisateur doit pouvoir être consulté par tout personnel du Cnous avec le niveau le plus élevé de visualisation du détail des occurrences[4].

Sur autorisation du chef d'établissement et au regard de ses fonctions, l'utilisateur peut cependant limiter la visibilité aux seules périodes de disponibilité et indisponibilité pour toute ou partie des personnels (sans le détail des rendez-vous–objet, lieu, …).

L'utilisateur peut également, s'il le souhaite, faire figurer des événements personnels sur son agenda avec la possibilité de les masquer à tout autre utilisateur (rendez-vous privé).

Dans l'objectif de réduire le nombre de sollicitations mails reçues par chacun, pour l'organisation d'une réunion avec d'autres utilisateurs du Cnous, l'utilisateur doit privilégier la consultation des agendas des autres personnels du Cnous devant être associés à la réunion avant de proposer un créneau adapté aux disponibilités du chacun pour confirmation.

Section 5.03 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'établissement.

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

Internet est un outil de travail réservé à un usage professionnel et, à titre résiduel, à un usage privé (tel que défini à l'article IV dans le respect de la législation en vigueur.

La consultation de sites contrevenants à la loi est donc strictement prohibée.

a) Publications sur les sites internet et intranet de l'établissement

Toute publication de pages d'information sur les sites internet ou intranet de l'établissement 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'établissement n'est autorisée, sauf disposition particulière précisée par l'établissement.

b) Sécurité

L'établissement se réserve le droit de filtrer ou d'interdire l'accès à certaines ressources numériques,

[4] L'utilisateur peut et doit vérifier que les autorisations de partage de son agenda sont bien positionnées.

de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes. L'utilisateur en est informé.

Section 5.04 RESEAUX SOCIAUX

Les réseaux sociaux externes à l'établissement occupent une place de plus en plus importante dans la sphère professionnelle.
Ils permettent à l'établissement et à chaque utilisateur de créer et de gérer les relations professionnelles et d'optimiser la communication et les actions « marketing ».

Dès lors que son appartenance à l'établissement transparait dans son utilisation d'un réseau social, l'utilisateur est informé que toute information publiée relative à l'établissement, son activité… relève d'une communication au sein de la sphère professionnelle.

Ainsi, dès lors que le réseau social est le support d'un usage professionnel, l'utilisateur doit :

- Utiliser un profil mettant explicitement en évidence son identité (nom, prénom, fonction…) ;
- Appliquer les mêmes règles d'usage et de déontologie que celles décrites dans les sections ci-dessus (notamment les sections 5.01 et 5.02) ;
- S'abstenir de créer un profil générique relatif à l'établissement ou une de ses activités sans autorisation explicite du directeur de l'établissement.

Section 5.05 TELECHARGEMENT

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

L'établissement se réserve le droit de limiter le téléchargement de certains fichiers pouvant présenter un risque (virus susceptibles altérer le bon fonctionnement du système d'information de l'établissement, codes malveillants, programmes espions, …).

Article VI. Accès à distance au système d'information

Un utilisateur exerçant ses activités dans un autre lieu que les locaux de l'établissement (télétravail) bénéficie des mêmes droits et est soumis aux mêmes obligations qu'un utilisateur travaillant sur site (tel que décrit dans la présente charte).

Il est admis un usage privé résiduel du matériel mis à disposition par l'établissement selon les dispositions de l'article IV. Avant tout usage privé, l'utilisateur a pour obligation :

- De veiller à la confidentialité et intégrité des données professionnelles afin qu'elles ne soient pas accessibles/modifiables par des tiers,
- De procéder à la déconnexion du réseau et de toutes les applications professionnelles (VPN, messagerie, intranet, etc.)

L'utilisateur veille tout particulièrement à ce que l'accès aux ressources numériques professionnelles (ordinateur, téléphone, …) soit, en son absence, verrouillé rendant l'utilisation impossible par toute autre personne.

Article VII. Traçabilité

L'établissement se réserve le droit de mettre en place des outils de traçabilité d'utilisation du système d'information. L'établissement est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées. Ces outils de traçabilité sont mis en œuvre suivant les recommandations de la Commission nationale de l'informatique et des libertés (CNIL), notamment la durée de conservation des traces.

Article VIII. Respect de la propriété intellectuelle

L'établissement rappelle que les systèmes d'information ne doivent, en aucune manière, être utilisés à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droitd'auteur ou par un droit voisin, tels que des textes, images, photographies, œuvres musicales, œuvres audiovisuelles, logiciels et jeux vidéo, sans l'autorisation des titulaires des droits prévues aux livres Ier et II du code de la propriété intellectuelle lorsque cette autorisation est requise.

Il est rappelé à cet égard que l'établissement, titulaire d'un accès à Internet, est tenu, de par la loi, à mettre en œuvre les moyens nécessaires que l'accès Internet ne soit pas utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin. La loi prévoit qu'en cas de non-respect de cette obligation, le titulaire de l'accès Internet peut voir sa responsabilité pénale engagée au titre de la négligence caractérisée.

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.

L'établissement pourra mettre en œuvre les mesures de contrôle appropriées au respect de cette clause.

Article IX. Respect du RGPD

Le 25 mai 2018, le règlement (UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (dit « règlement général sur la protection des données » - RGPD) est entré en application. Ce règlement, à l'instar de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, est applicable dès lors qu'un traitement met en œuvre un traitement de données à caractère personnel.

Dans le cadre de l'exercice de ses compétences, l'établissement est amené à collecter et traiter les données à caractère personnel. Conformément à la loi, les personnes concernées par les traitements de données à caractère personnel sont titulaires de droits sur l'usage qui peut être fait de ces données.

L'établissement a donc des obligations en la matière et instaure une politique de gestion de données à caractère personnel strictement conforme au RGPD. Il est rappelé notamment que la collecte et le traitement des données personnelles doivent être réalisés de manière strictement nécessaire et proportionnelle à l'objectif poursuivi.

Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée en coordination avec le délégué à la protection des données (DPO).

L'utilisateur doit notamment veiller :

- A respecter les dispositions imposées par le RGPD ;
- A mettre en œuvre les procédures validées par le DPO dans la transmission des données personnelles ;
- A signaler toute violation, ou tentative de concernant des données personnelles ;
- A se conformer aux règles en vigueur en matière notamment de collecte, de finalité, de durée de conservation, de sécurité et de confidentialité de données ;

En cas de difficulté sur le respect des dispositions du RGPD, l'utilisateur doit solliciter le délégué à la protection des données (DPO) qui lui apportera conseil et définira les procédures adaptées.

Article X. Entrée en vigueur de la charte

La présente charte entre en vigueur le …….. en remplacement de la précédente charte relative aux usages du système d'information