CHARTE DE BON USAGE DES RESSOURCES INFORMATIQUES A L'ÉCOLE NATIONALE SUPERIEURE D'ARTS & METIERS

Vu la circulaire n°2004-035 du 18 février 2004
Vu le code du travail ;
Vu le code de l'éducation ;
Vu le code pénal ;

Les ressources informatiques de l'École Nationale Supérieure d'Arts et Métiers (ENSAM) doivent être utilisées dans le respect de règles visant à garantir leur fonctionnement normal et la sécurité des systèmes d'information.

C'est dans ce contexte que l'ENSAM adopte la présente charte.

L'objectif de cette charte est de définir les conditions d'utilisation et les règles de bon usage des ressources informatiques de l'établissement par ses utilisateurs dans le cadre de leurs activités.

La charte précise les responsabilités de l'utilisateur conformément aux lois et règlements en vigueur dans le service public.

Elle intègre également les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ainsi que les dispositions relatives à la protection des données personnelles du Règlement Général sur la Protection des Données (RGPD).

Les règles énoncées dans la charte reflètent la volonté d'Arts et Métiers d'assurer un usage loyal, respectueux et responsable de ses ressources informatiques, tout en protégeant son patrimoine informatique et intellectuel.

La charte est annexée au règlement intérieur et a donc une valeur réglementaire. Elle s'applique à tous les utilisateurs.

Table des matières

1. Champ d'application

Les règles et obligations définies dans cette charte s'appliquent à tous les utilisateurs des ressources informatiques de l'Établissement.

Il est entendu par « utilisateur » toute personne quel que soit son statut ayant accès aux ressources informatiques de l'd'Arts et Métiers dans le cadre de ses activités. Sans que ce soit limitatif, l'utilisateur peut être un agent d'Arts et Métiers, un agent mis à disposition auprès d'Arts et Métiers, un(e) vacataire, un(e) intérimaire, un(e) stagiaire, un(e) étudiant(e), un(e) invité, visiteur ou l'employé(e) de société prestataire.

Sans que ce soit limitatif, il est entendu par « ressources informatiques », ou « systèmes informatiques » tout serveur, station de travail, ordinateur portable ou fixe (PC), matériel amovible (clés USB, disque dur externe, etc.) et l'infrastructure réseaux. Ces termes englobent également les applications, les bases de données et tout logiciel ou matériel affectés au fonctionnement du réseau d'Établissement ainsi que les services liés mis à disposition.

Sans que cela soit limitatif, les « moyens informatiques » désignent tout équipement informatique mis à disposition de l'utilisateur par l'Établissement notamment l'ordinateur portable ou fixe (PC), tablette, téléphone mobile, imprimante, etc.

2. Moyens informatiques

2.1. Accès aux moyens informatiques

Chaque utilisateur dispose d'un droit d'accès personnel lui permettant de s'identifier lorsqu'il utilise son poste de travail. Ce droit d'accès personnel est matérialisé sous forme de compte informatique qui comprend un identifiant et un mot de passe.

L'identifiant est généralement immuable alors que le mot de passe doit être changé régulièrement. Les règles de sécurité à suivre pour une gestion sécurisée des mots de passe et des contrôles d'accès sont annexées à la présente charte (Annexe 1 et 2).

Le droit d'accès d'un utilisateur à un système informatique est soumis à l'autorisation de la Direction des Systèmes d'Informations (DSI) d'Arts et Métiers. Un utilisateur peut demander un droit d'administration de sa machine ; ce droit lui est accordé après validation du responsable hiérarchique, du Responsable Informatique du Campus (RIC), du Responsable de la Sécurité des Systèmes d'Information (RSSI) et du Fonctionnaire Sécurité Défense (FSD).

Ce droit est limité à des activités conformes aux missions d'Arts et Métiers prévues dans son décret statutaire n°2012-1223 du 2 novembre 2012 modifié.

Il est personnel, incessible et disparaît lorsque les raisons de cet accès disparaissent.

Certains accès peuvent être suspendus en cas de cessation provisoire d'activité.
Cette suspension est réalisée manuellement à la demande de l'établissement.
Les accès peuvent concerner, de manière non exhaustive, des droits applicatifs, un droit d'administration, l'accès à la messagerie ou encore la totalité des accès informatiques.
La demande de l'établissement précisera le périmètre des droits à limiter. En cas d'arrêt longue maladie, l'établissement s'engage à conserver au minimum un droit d'accès à la messagerie.

En cas de cessation d'activité de longue durée, l'établissement peut laisser l'accès à la messagerie, à l'Intranet, au réseau social d'établissement et à la suite Office.

Certains accès peuvent être suspendus en cas de manquement répété aux règles de la présente charte informatique. Si cela s'avère possible en regard de la confidentialité, il sera précisé la justification de la demande.

2.2. Utilisation des moyens informatiques

2.2.1. Modalités de connexion

La connexion d'un matériel informatique au réseau est soumise à l'accord du service responsable et du Service Informatique du Campus (SIC) d'Arts et Métiers. L'installation d'application(s) et la modification de la configuration de l'ordinateur mis à disposition de l'utilisateur sont interdites sauf si elles sont réalisées par un personnel de la DSI ou par une personne ayant le droit administrateur.

L'utilisateur doit respecter les modalités de raccordement des matériels au réseau de l'Établissement. Tout ordinateur, devant être connecté au réseau, doit être déclaré au Service Informatique du Campus et doit être géré par un administrateur désigné (voir §10 ci-dessous). Ce dernier doit en particulier s'assurer que les règles de sécurité et de confidentialité sont bien respectées.

2.2.2. Propriété des moyens informatiques

Les moyens informatiques mis à la disposition de l'utilisateur restent la propriété de l'Établissement.

L'Établissement reste seul propriétaire de tous les supports mis à disposition des utilisateurs, notamment les supports physiques (disques durs, supports USB et optiques, etc.) et les accès à des espaces de stockage en ligne mis à disposition par l'ENSAM.

L'accès à ces supports pourra être restreint par l'Établissement sans préavis (voir §2.1 ci-dessus). Si cela s'avère possible en regard de la confidentialité, il sera précisé la justification de la demande.

2.2.3. Restitution du matériel en cas de départ ou changement de matériel

Lorsque les raisons d'octroi des moyens informatiques disparaissent, l'utilisateur doit les restituer.

En cas de départ de l'Établissement, ces moyens informatiques devront être restitués le dernier jour travaillé ou de présence et, à la demande, dans les 15 jours suivants le dernier jour travaillé. Par dérogation justifiée, ce délai peut être supérieur à 15 jours après accord de la DSI. Dans tous les cas, la restitution d'un ou de plusieurs matériels fera l'objet d'un document actant les éléments restitués ou manquants. Une copie de ce document sera fournie à l'agent ainsi qu'à la Direction des Ressources Humaines (DRH).

En cas de changement de matériel informatique (ordinateur, téléphone portable, etc.) par un matériel plus récent, l'utilisateur doit restituer l'ancien matériel dès la mise en service du nouveau ou, au plus tard, sur demande dérogatoire validée par la DSI, 15 jours après.

Sur simple demande écrite, l'établissement peut demander la restitution des moyens informatiques confiés à l'agent. Si cela s'avère possible en regard de la confidentialité, il sera précisé la justification de la demande.

2.3. Inventaire des moyens informatiques de l'établissement et protection du SI

Afin de respecter les règles comptables et la sécurité des réseaux, l'Établissement doit connaître exhaustivement l'ensemble des moyens informatiques et logiciels informatiques qu'il met à disposition des utilisateurs.

A ce titre, il est porté à la connaissance des utilisateurs qu'un outil de récupération des informations matériels et logiciels ainsi que des outils de protection sont installés sur tous les postes de l'Établissement.

Ces outils collectent toutes les informations matérielles et logicielles de l'ordinateur et vérifient, contrôlent la sécurité du poste et chiffrent les données.
Ces outils ne permettent pas d'accéder aux données professionnelles et/ou privées des utilisateurs.

Tous les postes de l'Établissement sont concernés par cette mesure, qu'il s'agisse de poste dit Administratifs ou de Laboratoires, sous un système Windows ou Linux (ou autre). Dans le cas où ces outils généreraient un disfonctionnement, une étude sera menée par la DSI pour identifier la meilleure solution permettant de protéger le poste tout en assurant le service.

Les moyens informatiques achetés par d'autres entités (AMVALOR, CNRS, INRA, entreprise privée, etc.) doivent être dotés des outils d'Arts et Métiers s'ils sont connectés au réseau privé de l'Établissement. A défaut, ces postes pourront utiliser le réseau invité.

Chaque utilisateur a un devoir d'alerte auprès du Service Informatique du Campus et du Responsable de la Sécurité du Système d'Information (RSSI) en cas, notamment, d'intrusion ou de tentative d'intrusion dans l'ordinateur mis à sa disposition, ou de suspicion de présence d'un virus ou de tout autre logiciel malveillant.

Les utilisateurs ont l'obligation de scanner tous les supports amovibles (clé USB, CD, DVD, disques, etc.) qu'ils apportent au sein de l'établissement sur des ordinateurs spécifiques prévus pour cet usage, dites stations blanches, qui sont à disposition sur tous les campus.

Les utilisateurs de matériels informatiques portables s'engagent, quel que soit l'endroit où ils se trouvent, à sécuriser le matériel informatique de l'Établissement et l'accès aux données qu'il contient selon les règles de sécurité en vigueur (Annexe 1 et 2). Il est entendu par « matériels informatiques portables », sans que la liste ne soit limitative, les ordinateurs portables, les assistants numériques personnels (PDA), les tablettes et les téléphones mobiles, mis à disposition par l'Établissement.

Les données sensibles ou stratégiques pour l'Établissement transportées par les utilisateurs sur des matériels informatiques portables devront être chiffrées. A la demande et auprès du RSSI, un outil de chiffrement est mis à disposition des utilisateurs. Il en est de même pour les données sensibles ou stratégiques qui pourraient être stockées sur des clés USB et autres supports de stockage (disque dur amovible, CD, DVD, etc.).

3. Propriété et confidentialité des informations

3.1. Principes généraux

Les fichiers créés ou possédés par chacun des utilisateurs qui sont stockés dans les systèmes ou moyens informatiques mis à disposition doivent être considérés comme des fichiers de l'Établissement dans les limites des règles de titularité énoncées dans le Code de la Propriété Intellectuelle (CPI).

Ainsi en matière de droit d'auteur hors logiciel (texte, vidéo, audio…) :

- Concernant les enseignants, enseignants chercheurs, Professeurs Agrégés (PRAG), Professeurs Certifiés (PRCE), Attachés Temporaires d'Enseignement et de Recherche (ATER) et les doctorants contractuels effectuant une mission d'enseignement, ces derniers sont propriétaires de leurs créations.
- Concernant les autres agents de l'Établissement (personnel, ingénieur administratifs, techniques, ouvriers, et de service) leurs créations sont cédées à l'ENSAM, ils pourront voir leurs œuvres utilisées par l'ENSAM et ne pourront s'opposer à la modification de leurs œuvres si les conditions pour appliquer ces dérogations sont réunies conformément au Code de la Propriété Intellectuelle (CPI). Dans le cas où l'ENSAM souhaite exploiter commercialement les œuvre desdits agents, un contrat de cession de droits d'auteur devra être signé entre l'ENSAM et le(s)dit(s) agent(s) prévoyant notamment une contrepartie financière selon les dispositions de l'article L131-3-1 du CPI.
- Concernant les étudiants ces derniers restent toujours propriétaires de leurs œuvres.

Ainsi en matière de logiciel et documentation associée :

- Concernant l'ensemble des agents d'Arts et Métiers quel que soit leur statut, ses stagiaires ou encore ses professeurs émérites l'Établissement est propriétaire par principe si les conditions sont réunies conformément au CPI et reversera à(aux) l'auteur(s) une prime d'intéressement selon les dispositions du décret n°96-858 du 2 octobre 1996.
- Concernant les étudiants ces derniers restent toujours propriétaires des logiciels et documentations associée.

Ainsi en matière d'inventions :

- Concernant l'ensemble des agents d'Arts et Métiers quel que soit leur statut, ses stagiaires ou encore ses professeurs émérites, l'Établissement est propriétaire par principe si les conditions sont réunies conformément au CPI et reversera à(aux) l'inventeur(s) une rémunération supplémentaire conformément à l'article L611-7 du CPI.
- Concernant les étudiants ces derniers restent toujours propriétaires de leurs inventions.

Concernant les fichiers stockés dans les systèmes informatiques, provenant de tierces personnes notamment des partenaires, et de manière générale de personnes extérieures hors étudiants et personnel d'Arts et Métiers, leur propriété n'est pas affectée sauf dispositions contractuelles contraires.

Dans le cadre de ses activités professionnelles, lorsque l'utilisateur stocke sur son ordinateur des fichiers qui lui sont personnels, il doit les identifier de façon explicite comme étant « personnel ». La nature personnelle d'un document peut figurer dans son nom ou dans le nom du répertoire dans lequel il est stocké. A défaut, les documents sont présumés être de nature professionnelle et accessible par l'établissement.

Stocker des fichiers personnels doit rester marginal et engage la responsabilité de l'utilisateur, notamment en cas d'intrusion d'un virus ou de tout autre logiciel malveillant.

Dans le cadre de ses activités professionnelles, lorsque l'utilisateur stocke sur son ordinateur des fichiers qui sont confidentiels vis-à-vis d'industriels, il doit les identifier de façon explicite comme étant « confidentiel ». La nature confidentielle d'un document peut figurer dans son nom ou dans le nom du répertoire dans lequel il est stocké. A défaut, les documents sont présumés être de nature professionnelle et accessible par l'établissement.

3.2. Cas des fichiers, dossiers partagés et Teams

Il est rappelé aux utilisateurs de dossiers partagés, d'équipes et de conversations Teams que tout document qui y est stocké peut généralement être lu, modifié et supprimé par les autres utilisateurs de ce dossier ou équipe Teams. Par souci de sécurité, il est demandé aux utilisateurs de ne pas y stocker des dossiers personnels ou confidentiels et de veiller au contenu des conversations. Au sein d'une équipe Teams, seuls les personnels déclarés dans l'équipe peuvent avoir accès au contenu de l'équipe. Au sein d'un canal privé d'une équipe Teams, seuls les personnels déclarés dans ce canal peuvent avoir accès au contenu du canal.

Dans le cadre d'activités professionnelles, lorsqu'il s'agit de fichiers créés par un utilisateur employé par Arts et Métiers et déclarés partagés entre plusieurs tutelles dûment définies, leur accès est réservé aux membres du personnel de celles-ci selon des modalités soumises à l'approbation de leur créateur.

3.3. Cas des fichiers et dossiers partagés pour les syndicats et instances

Pour toutes les personnes participantes aux syndicats, tous les documents ou dossiers liés à cette activité syndicale devront porter le libellé « personnel » afin que les administrateurs ne puissent pas y accéder. Par ailleurs, tous les documents élaborés dans le cadre des différentes instances devront être classés dans des dossiers avec le libellé « confidentiel » pour les mêmes raisons.

4. Propriété intellectuelle

Il est interdit à tout utilisateur de copier les logiciels installés sur les moyens informatiques.

Il est interdit à tout utilisateur d'installer un logiciel ou supprimer les logiciels installés, sur les moyens informatiques pour quelque usage que ce soit, à l'exclusion des personnes ayant les droits administrateurs.

Tout utilisateur doit se conformer aux prescriptions d'utilisation définies dans la licence par l'auteur et/ou le fournisseur d'un logiciel. Il est strictement interdit de modifier un logiciel.

Il est strictement interdit d'installer un logiciel sur un moyen informatique sans s'être assuré préalablement que les droits de licence le permettent.

En cas de détection d'installation illégale d'un logiciel à partir du réseau informatique de l'Établissement, celui-ci se réserve le droit de couper l'accès réseau du poste incriminé, qu'il appartienne à l'Établissement ou non, et cela jusqu'à suppression des licences illégales.
L'utilisateur sera informé dès que possible par tous les moyens à la disposition de l'établissement.

Le téléchargement massif et systématique de ressources documentaires par l'intermédiaire d'un robot ou de tout autre logiciel est interdit.

5. Protection des données à caractère personnel

Le traitement de données à caractère personnel réalisé par l'utilisateur dans le cadre des activités d'Arts et Métiers doit respecter les dispositions de la loi Informatique et Liberté du 6 janvier 1978 modifiée et du 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, et abrogeant la directive 95/46/CE dit « Règlement Général sur la Protection des Données (RGPD) ».

Un fichier ou un logiciel nécessitant l'utilisation de données à caractère personnel constituent des traitements de données à caractère personnel soumis au cadre législatif et règlementaire précité. Ces traitements doivent être autorisés par le responsable pédagogique ou hiérarchique et être déclarés auprès du Délégué de la Protection des Données (DPD) ou, en anglais, Data Protection Officer (DPO), d'Arts et Métiers le plus tôt possible et préalablement à leur mise en place.

Le DPO peut être contacté par voie électronique à l'adresse dpo@ensam.eu ou par voie postale à l'adresse ENSAM SJPI&C – DPO 151 boulevard de l'hôpital 75013 Paris.

6. Modalités d'utilisation des moyens informatiques

6.1. Principes généraux d'utilisation

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques mises à disposition et s'engage à ne pas effectuer des opérations qui pourraient entraver et/ou endommager le fonctionnement normal du réseau, l'intégrité du système informatique et les flux internes et/ou externes de l'Établissement.

Chaque utilisateur est tenu pour responsable de toute utilisation des ressources informatiques faite à partir de son compte informatique. Lorsque l'utilisation d'un système informatique implique l'ouverture d'un compte nominatif, l'utilisateur ne doit pas se servir, pour y accéder, d'un autre compte que celui qui lui a été attribué par l'administrateur habilité.

De manière général, l'établissement ne peut pas imposer à un agent un usage professionnel d'un matériel personnel.

L'Établissement ne prend pas en charge la sauvegarde des fichiers et des données locales situés sur le disque dur de l'ordinateur, qu'il soit fixe ou portable. Pour sauvegarder vos données, il est recommandé de les placer sous OneDrive.

L'usage professionnel des réseaux sociaux (WhatsApp, Messenger, Facebook, etc.) est interdit sauf dérogation validée par l'Établissement.

6.2. Le droit à la déconnexion

Le droit à la déconnexion reconnaît le droit fondamental des agents de se déconnecter de leurs outils numériques en dehors des heures de travail définies dans les fiches horaires annuelles individuelles, favorisant ainsi un équilibre entre vie professionnelle et vie personnelle.
La mise en œuvre de ce droit se traduit par la définition et la mise en œuvre de bonnes pratiques. Ces dispositions concernent notamment les réunions, les appels téléphoniques, ainsi que les envois de SMS et de mails.

Ainsi, dans le but de respecter le droit à la déconnexion de chaque agent, il est, sauf urgence, circonstances exceptionnelles ou astreintes, recommandé de :

- Ne pas planifier ou débuter une réunion avant 9h ou après 17h et éviter les réunions sur les horaires de pause méridienne.
- Ne pas passer d'appels téléphoniques en dehors des horaires habituels de son service de rattachement, pendant les jours de repos hebdomadaires ou pendant les congés des agents. Cela s'applique aussi à l'envoi de SMS.
- Ne pas envoyer de mails en dehors des horaires habituels de son service de rattachement et notamment pendant le week-end. Pour mémoire, il est possible de préparer en amont ses messages et de différer leur envoi pendant les heures habituelles de travail. La messagerie électronique permettant de consulter ses mails en dehors de l'établissement, nous rappelons qu'il n'y a aucune obligation de répondre en temps réel aux mails reçus en dehors des horaires habituels de travail, pendant les jours de repos hebdomadaires ou les congés.

La Direction et les managers d'Arts et Métiers seront particulièrement attentifs au respect de ces mesures afin de garantir l'application du droit à la déconnexion, et contribuer ainsi à l'amélioration de la qualité de vie au travail au sein de l'institution.

6.3. Utilisation de la messagerie électronique

Les utilisateurs de l'Établissement disposent d'une messagerie électronique personnelle. L'utilisation à des fins personnelles de cet outil est tolérée à condition qu'elle n'affecte, ni la performance et la sécurité des réseaux de l'Établissement, ni la productivité des utilisateurs.

Il est rappelé qu'aucune garantie de bonne réception ne peut être exigée pour les emails.

L'utilisateur est informé par la présente charte de la mise en place au sein de l'Établissement d'un dispositif de filtrage, d'analyse et de détection de logiciels malveillants, des spams, au sein des messages.

6.3.1. Accès à la messagerie

Seuls l'utilisateur et les administrateurs systèmes de la DSI peuvent avoir accès à la messagerie.
L'accès au contenu de la messagerie d'un utilisateur par un administrateur n'est réalisé qu'à la demande de l'usager ou sur demande de la justice.

6.3.2. Utilisation personnelle de la messagerie électronique

Tout utilisateur doit gérer prudemment sa messagerie électronique.

Il est rappelé que l'usage de la messagerie à titre personnel doit rester compatible avec les activités de l'Établissement. Cet usage ne doit pas avoir des conséquences néfastes sur le fonctionnement normal du réseau ou sur l'intégrité de l'outil informatique. En particulier, est proscrit l'envoi de messages à caractère personnel en diffusion générale.

Le bon usage normal de la messagerie implique de respecter plusieurs règles présentées à l'Annexe 3.

6.3.3. Utilisation associative de la messagerie électronique

Les associations de personnel bénéficient d'une adresse mail professionnelle dédiée à la fonction associative ou syndicale et ils doivent utiliser la messagerie dans le respect des règles de la présente charte.
Elles doivent faire un usage normal de la messagerie et ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement normal du réseau ni sur l'intégrité de l'outil informatique.
Le caractère associatif du message doit être indiqué dans l'objet. La signature du mail doit faire apparaître la fonction au sein de l'association. En ce qui concerne les utilisateurs employés par Arts et Métiers, en aucun cas, la fonction professionnelle au sein de l'Établissement ne doit apparaître.

Tout envoi d'un message à contenu associatif notamment en diffusion générale, doit se faire par l'intermédiaire de l'adresse de messagerie créée pour chaque association.

L'utilisation d'une liste de diffusion générale pour envoyer un message de nature associative est licite. Néanmoins, les associations de personnel doivent indiquer en fin de message la possibilité, pour les destinataires, de demander à tout moment à être radiés de cette liste de diffusion. La création et la gestion des listes de diffusion doivent être réalisées par les associations ou syndicats.

6.3.4. Utilisation syndicale de la messagerie électronique

L'utilisation par les organisations syndicales des technologies de l'information et de la communication dans la fonction publique de l'Etat est encadrée par l'arrêté du 4 novembre 2014 relatif aux conditions générales d'utilisation par les organisations syndicales des technologies de l'information et de la communication dans la fonction publique de l'Etat, (Article 8), et est applicable au sein de l'Établissement.

6.4. Utilisation d'Internet et sites Internet

Les utilisateurs disposent d'un accès à Internet. Une utilisation personnelle de l'accès Internet est tolérée à condition qu'elle n'affecte pas la sécurité des réseaux de l'Établissement, ni la productivité des utilisateurs.

Sont considérés comme étant à caractère illicite tout contenu défendu par la loi, notamment les contenus à caractère pédophile, d'incitation à la haine raciale, au terrorisme, etc. La visualisation, la récupération, le stockage et la diffusion de contenus à caractère illicite constituent une violation de la présente charte. Ces actes peuvent également constituer des délits donnant lieu à des sanctions pénales.

Dans le cadre de leurs activités professionnelles, les utilisateurs s'engagent à respecter le principe de neutralité du service public, de l'Enseignement Supérieur et de la Recherche ainsi que l'ensemble des obligations qui s'imposent aux agents de l'Etat (obligation de réserve, obligation de discrétion professionnelle, secret professionnel, non-discrimination, neutralité, probité, etc.).

Toutes les publications sur les sites Internet de l'Établissement engagent la responsabilité de l'Établissement. Sont considérés comme des sites Internet de l'Établissement : l'Intranet, le site institutionnel, les sites Internet des laboratoires et tout autre site Internet portant le logo de l'Établissement ou décrivant explicitement son appartenance à l'Établissement.
L'utilisateur s'engage à ne pas publier de propos sur les sites Internet d'Arts et Métiers et/ou en étant identifié comme un agent d'Arts et Métiers, pouvant constituer notamment les délits d'injure, de diffamation, de calomnie, de dénigrement et d'atteinte à la vie privée.

L'utilisateur s'engage à ne pas utiliser volontairement les services Internet pour la diffusion de logiciels malveillants, message publicitaire en masse, chaîne de lettre ou de mailing personnel.

L'utilisateur est informé par la présente charte que l'Établissement met en place un dispositif permettant d'interdire la consultation de sites non autorisés dont la liste évolue constamment. Cette liste peut contenir des sites légalement interdits comme, par exemple, ceux traitant de l'apologie du terrorisme ou violant la propriété intellectuelle.

Afin d'assurer le bon fonctionnement des applications et permettre un accès rapide aux données, l'Établissement peut interdire ou limiter l'accès à certains sites internet trop consommateur de bande passante, même s'ils sont licites.

6.5. Utilisation du téléphone mobile mis à disposition par l'établissement

L'utilisation du téléphone mobile professionnel est réservée prioritairement aux appels à caractère professionnel et usages professionnels.
L'utilisation personnelle ne doit pas occasionner de frais supplémentaires pour l'Établissement.

6.6. Utilisation d'un réseau externe

6.6.1. Principes généraux

Les dispositions de la Charte s'appliquent à l'utilisateur qui se connecte au système informatique en dehors des locaux d'Arts et Métiers avec ou sans matériels informatiques mis à disposition par l'établissement.

6.6.2. Télétravail

Dans le cadre de la convention de télétravail, l'agent accepte de mettre à disposition sa box, sa liaison internet, ses câbles ou son Wifi pour permettre la connexion de l'ordinateur professionnel au système d'information de l'Établissement.
Lorsque l'utilisateur est employé par Arts et Métiers et bénéficie du télétravail, il doit assurer la confidentialité, l'intégrité et la disponibilité des informations qui lui sont confiées ou auxquelles il a accès dans le cadre professionnel, par l'emploi des moyens informatiques d'Arts et Métiers.
Il est rappelé explicitement que, dans le cadre du télétravail, l'usage de l'ordinateur professionnel est strictement limité à l'agent et que nulle autre personne ne doit l'utiliser. Il est à la charge de l'usager de veiller à ne pas laisser l'ordinateur connecté et sans surveillance. La session de l'utilisateur doit être systématiquement verrouillée lorsque l'ordinateur n'est plus utilisé.

6.7. Clôture des comptes utilisateurs

En application de l'article 34-1 du CPCE, il existe une clôture des comptes des utilisateurs après leur départ de l'Établissement.

Sauf demande contraire de l'Établissement en accord avec l'agent, la clôture des comptes des agents est effectuée un an après la fin du contrat les liant à l'Établissement.
L'agent quittant l'Établissement et son responsable hiérarchique s'informent mutuellement et se mettent d'accord sur le devenir des fichiers et données existants et informent le Service Informatique du Campus.
L'absence d'information auprès du Service Informatique du Campus risque de provoquer un nettoyage systématique des données disponibles et une perte de données irréversible.

Ainsi qu'il est précisé à l'article 4 de la présente charte, les utilisateurs employés par Arts et Métiers qui ne sont pas propriétaires des fichiers informatiques produits durant leurs activités au sein de l'Établissement doivent lors de leur départ s'assurer que ces informations restent disponibles et utilisables par l'Établissement.

7. Enregistrement des flux de données entrantes et sortantes

Pour des nécessités de sécurité et de bon fonctionnement des moyens informatiques, l'utilisateur est informé de la mise en place d'un enregistrement automatisé de l'ensemble des flux d'information circulant sur le réseau de l'Établissement.

Il s'agit d'un traitement de données à caractère personnel destiné à contrôler les connexions effectuées par les utilisateurs à leur messagerie professionnelle et à Internet. Le traitement est opéré à partir des données d'identification prévues aux articles R10-12 et R10-13 du Code des postes et des communications électroniques (CPCE).

Ce contrôle de l'utilisation des ressources informatiques est réalisé dans le respect de la loi n°78-17 du 6 janvier 1978 modifiée et du RGPD (article 6-1-c). Il est fondé sur le respect des obligations légales et réglementaires de conservation desdites données prévues aux article L 34-1 et R10-13 du CPCE.

Leur durée de conservation par l'Établissement est d'une durée maximale de 6 mois ou de 1 an en cas de chiffrement des données.

Aucun transfert hors de l'Union Européenne n'est réalisé.

Les données à caractère personnel conservées sont accessibles aux seules personnes spécifiquement habilitées de la DSI et seulement sur ordre de la justice et de la police. La DSI n'a un droit d'accès seulement pour transférer ces données aux ayants droit judiciaire.

Les utilisateurs disposent d'un droit d'accès, de rectification, de limitation, d'opposition, d'effacement et de portabilité sur les données à caractère personnel les concernant à l'exception des données concernant la circulation du flux d'information. Ils peuvent exercer ces droits auprès du DPO. Le DPO peut être contacté par voie électronique à l'adresse dpo@ensam.eu ou par voie postale à l'adresse ENSAM SJPI&C – DPO 151 boulevard de l'hôpital 75013 Paris. Les modalités de saisine du DPO sont précisées en Annexe 5 de la présente charte.

8. Mesures conservatoires et sanctions

8.1. Mesures conservatoires

Les administrateurs peuvent prendre des mesures conservatoires si l'urgence l'impose, notamment en cas de danger prévisible pour les systèmes d'information ou s'il existe une présomption sérieuse de non-respect de la charte.

Les directeurs et chefs de services peuvent prendre des mesures conservatoires, dans l'attente de la saisine éventuelle du conseil de discipline à l'égard des agents non respectueux des règles de sécurité, en restreignant l'accès aux outils informatiques.

8.2. Sanctions

Le non-respect des dispositions de la présente charte ainsi que des textes de loi en vigueur peut exposer le contrevenant à des sanctions administratives, civiles ou pénales, les unes n'étant pas exclusives des autres.

9. Droits et devoirs spécifiques de l'Établissement

L'Établissement fera ses meilleurs efforts pour s'assurer du respect par les utilisateurs des règles de bonne utilisation des moyens informatiques.

L'Établissement ne pourra être tenu pour responsable des agissements qui sont imputables à l'utilisateur qui ne se serait pas conformé à l'ensemble des règles énoncées dans la présente charte. Si ces agissements sont commis par un agent, cette limitation de responsabilité de l'Établissement ne s'applique qu'en cas de faute lourde personnelle détachable du service.

Dans le cadre professionnel, les éventuels dysfonctionnements qui pourraient survenir pendant l'usage des applications nécessaires à l'exercice des missions de l'utilisateur ne sauraient constituer, à eux seuls, un motif d'interruption de travail.

L'établissement dote ses personnels des moyens informatiques adaptés à leur fonction.

10. Droits et devoirs des administrateurs

Les administrateurs des systèmes informatiques ont le devoir d'assurer un bon fonctionnement des moyens informatiques mis à disposition des utilisateurs et cela dans la limite des moyens octroyés par l'Établissement.

Le terme « administrateur » désigne un professionnel qui a pour métier de gérer techniquement, d'exploiter, de configurer, de maintenir, de sécuriser une ressource informatique. Il dispose de droits étendus permettant l'accès à des informations à caractère personnel d'autres utilisateurs (informations nominatives, données personnelles, traces, etc.). Il en existe de différents types, selon la ressource qu'il a à gérer : administrateur réseau, administrateur système, administrateur messagerie, administrateur de bases de données, administrateur de site web, administrateur fonctionnel, etc.

Les administrateurs ont l'obligation de préserver la confidentialité des données à caractère personnel, au sens de la loi informatique et libertés du 6 janvier 1978 modifiée et du RGPD, ainsi que les informations confidentielles qu'ils sont amenés à connaître dans le cadre de l'exercice de leurs fonctions à des fins de diagnostic et d'administration des systèmes (traces, fichiers, contenu de bases de données, en-têtes de messages, etc.).
Ils ne doivent pas accéder aux messages, dossiers et fichiers identifiés comme personnels ou confidentiels par les utilisateurs, sauf en cas d'injonction de l'autorité judiciaire ou accord des utilisateurs.
Par la présente charte, les utilisateurs sont informés de l'existence au sein de l'Établissement de logiciels de prise en main à distance utilisés strictement à des fins de maintenance informatique. La prise en main à distance ne peut être opérée qu'après acceptation de l'agent.

Les opérations de maintenance réalisées par les administrateurs sont tracées.

Les administrateurs informent les utilisateurs de toute modification de leurs droits d'accès et les sensibilisent, en coopération avec le RSSI, aux problèmes de sécurité inhérents aux systèmes d'information de l'Établissement.

Les administrateurs prennent les dispositions nécessaires pour faire respecter les exigences de la présente charte dans le respect des lois et règlements en vigueur.

Les administrateurs ont le devoir d'informer le RSSI et/ou le FSD de toute intrusion détectée sur les systèmes qu'ils administrent et de tout comportement dangereux d'un utilisateur.
Dès qu'une violation de données à caractère personnel est identifiée, le RSSI en informe le FSD, le DPO et l'Autorité Qualifiée de Sécurité des Systèmes d'Information (AQSSI), représentée par le Directeur Général.

Les administrateurs doivent mettre à la disposition de l'AQSSI et/ou du RSSI et/ou du FSD et/ou du DPO, et à leur(s) demande(s), leurs compétences pour rechercher l'origine de l'intrusion informatique et/ou de la violation de données.

11. Système d'information et utilisateurs utilisant des informations classifiées et ZRR

Conformément aux dispositions de l'instruction générale interministérielle n° 1300 / SGDN / PES / SSD du 25 août 2003 sur la protection des secrets de la défense nationale, les systèmes, les données et les utilisateurs concernés font l'objet de mesures particulières de sécurité en plus de celles figurant dans la présente charte.

Conformément aux dispositions régissant les Zones à Régime Restrictif (ZRR), les systèmes, les données et les utilisateurs concernés peuvent faire l'objet de mesures particulières de sécurité en plus de celles figurant dans la présente charte.

12. Information des utilisateurs

La présente charte est consultable sur le site Intranet de l'établissement et, sur demande, par remise d'un exemplaire papier soit :

- Auprès du service de la Scolarité ;
- Lors de la signature du contrat de travail ou du procès-verbal d'installation auprès de la Direction des Ressources Humaines de la Direction générale ou du campus concerné.

13. Entrée en vigueur

La présente charte entre en vigueur dès le lendemain de sa publication sur le site Intranet de l'Établissement.

Fait à Paris, le

Le directeur général
de l'École Nationale Supérieure
d'Arts et Métiers

Laurent CHAMPANEY

Fait le 08/07/2024

Laurent CHAMPANEY

Signé par Laurent CHAMPANEY

Signé et certifié par yousign

ANNEXE 1

Règles de bonne pratique

Chaque utilisateur doit respecter les consignes des administrateurs et des responsables informatiques, notamment celles qui concernent l'ouverture et la fermeture de compte informatique lors de l'arrivée et du départ définitif de l'utilisateur.

Accès à la session :

L'utilisateur ne quitte jamais son poste de travail en laissant une session ouverte ;

L'utilisateur s'assure que le mécanisme de verrouillage systématique du poste de travail est enclenché au-delà d'une courte période d'inactivité.

Mots de passe :

L'utilisateur choisit des mots de passe sûrs respectant les recommandations en la matière ;

L'utilisateur ne les communique jamais à un tiers y compris à un administrateur ;

L'utilisateur veille à ce que ses mots de passe soient tenus secrets ;

Il est fortement recommandé de ne pas les écrire sur un document papier ;

L'utilisateur est tenu à changer régulièrement ses mots de passe.

Utilisation raisonnable des ressources :

L'utilisateur use raisonnablement de toutes les ressources partagées (notamment, puissance de calcul, espace disque, jetons logiciels, bande passante sur le réseau, visioconférence, etc.) ;

En particulier, l'utilisateur doit se garder strictement :

- d'interrompre le fonctionnement normal du réseau ou des systèmes connectés au réseau (notamment : manipulations anormales, débranchement ou arrachement de câble, introduction de logiciels malveillants, etc.) ;
- de se connecter ou d'essayer de se connecter sur un site extérieur à l'Établissement sans s'être assuré de l'objet du site et notamment du fait qu'il n'est pas réputé illicite (par exemple, sites pédophile, d'incitation à la haine raciale, etc.) ;
- de télécharger ou lire des fichiers (sons, images, vidéos, etc.) sans rapport avec l'activité professionnelle ;
- d'accéder au compte d'un autre utilisateur sans l'autorisation de celui-ci ;
- d'accéder à des informations appartenant à d'autres utilisateurs du réseau, sans leur autorisation ;
- de modifier ou détruire des informations appartenant à d'autres utilisateurs et ceci sans leur autorisation
- de porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants ;

- de masquer sa véritable identité, en particulier en se connectant au réseau sous le nom d'un autre utilisateur ;
- de développer ou d'installer des outils mettant sciemment en danger l'intégrité des systèmes ;
- de nuire à l'image de marque de l'Établissement par une mauvaise utilisation des ressources informatiques mises à disposition.

Sécurité et confidentialité des données :

L'utilisateur verrouille son ordinateur dès qu'il quitte son poste de travail ;

L'utilisateur protège ses fichiers, avec l'aide éventuelle des administrateurs ;

L'utilisateur est responsable des droits qu'il accorde à des tiers sur ses documents ;

L'utilisateur contrôle l'accès des locaux où sont situés des équipements informatiques ;

L'utilisateur ne prête jamais son compte informatique ;

L'utilisateur veille à ce que ses fichiers soient régulièrement sauvegardés. Pour cela, il est très fortement recommandé de déposer ses fichiers sur OneDrive. L'Établissement ne pourra pas être tenu pour responsable des pertes ou détérioration de fichiers situés sur l'ordinateur professionnel de l'usager.

Signalement des problèmes :

L'utilisateur doit signaler au RSSI toute violation, tentative de violation ou toute violation suspectée d'un système informatique.

L'utilisateur signale aux administrateurs informatique et/ou au RSSI tout problème observé (mauvaise gestion des protections, faille système, logiciel suspect, message douteux, etc.) pouvant nuire au bon niveau de sécurité.

Respect des modalités de raccordement des matériels informatiques externe :

Tout utilisateur doit respecter les modalités de raccordement des matériels au réseau de l'Établissement. Ces modalités sont établies par la DSI.
Tout ordinateur, devant être connecté au réseau, doit être déclaré au Service Informatique du Campus et doit être géré par un administrateur désigné. Ce dernier doit en particulier s'assurer que les règles de sécurité et de confidentialité sont bien respectées.

L'utilisateur utilise de façon prudente les clés de stockage USB personnelles ainsi que tout autre support (tous supports amovibles) afin, notamment, de ne pas répandre des logiciels malveillants dans le réseau informatique de l'Établissement.

Avant d'être utilisé dans l'Établissement, tous les supports amovibles doivent être analysés sur des ordinateurs spécifiques prévus pour cet usage, dites stations blanches, présents au sein de chaque campus.

Il est recommandé aux utilisateurs de ce type de stockage de limiter le nombre des fichiers présents et de ne pas y conserver des fichiers sensibles.

ANNEXE 2

Règles de sécurité supplémentaires en cas de déplacement à l'étranger

Extrait de « SÉCURITÉ NUMÉRIQUE BONNES PRATIQUES À L'USAGE DES PROFESSIONNELS EN DÉPLACEMENT » réalisé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en 2019 :

https://www.ssi.gouv.fr/uploads/2014/09/anssi_passeport_2019_1.0.pdf

1. Évitez le transport de données superflues

- Minimiser le volume de données à emporter
- Chiffrer les données dans la mesure du possible
- Utiliser un cloud privé et sécurisé d'Arts et Métiers.

2. S'informer sur la législation du pays de destination AVANT PENDANT APRÈS

- Se renseigner auprès du service de la scolarité sur la législation en matière de protection des données dans le pays de destination
- Adapter la sécurisation des moyens de communication et de stockage au cadre réglementaire local et aux besoins de votre mission

3. Sauvegarder les données que vous emportez

- Réaliser des sauvegardes régulières sur un support fourni par l'Établissement déconnecté de tout réseau

4. Faire preuve de discrétion

- Éviter autant que possible la consultation de documents sensibles depuis des lieux publics et faire doter les équipements (ordinateur, tablette, téléphone) d'un filtre de confidentialité par la DSI.

5. Éviter de laisser vos documents et équipements sans surveillance

- En cas d'absence, même pendant un temps très court, verrouillez votre session de travail. Des enveloppes inviolables et câbles antivol pour ordinateurs portables existent et permettent de préserver leur intégrité en cas de séparation des équipements. Les enveloppes sont à disposition auprès du FSD de l'établissement.

Les câbles antivols sont à disposition auprès des supports informatique de campus.

6. Éviter de vous connecter aux réseaux ou équipements non maîtrisés

- Utilisez les moyens professionnels sécurisés fournis par votre organisation (téléphone, ordinateur, VPN, etc.). Ne les contournez pas par l'usage de moyens personnels (ex. : messagerie personnelle).
- Lorsque c'est possible, évitez de vous connecter aux réseaux non maîtrisés (Wi-Fi d'hôtel, de gare ou de café, bornes de recharge en libre-service, salle de réunion extérieure, etc.) et gardez votre pare-feu actif.
- N'utilisez pas les équipements qui vous sont offerts (clé USB, objet connecté, etc.) sans les avoir fait vérifier par la DSI, ils peuvent avoir été piégés.

7. Informer le Service Informatique du Campus , le FSD et RSSI en cas de perte ou vol

- En cas de disparition d'un équipement, informer sans délai le Service Informatique du Campus, le FSD et le RSSI. Ils pourront ainsi prendre sans délai les mesures nécessaires pour protéger l'Établissement.

8. Renouveler les mots de passe utilisés lors de votre déplacement

- Lorsque les équipements et applications le permettent, préférer l'authentification forte par application mobile.
- Utiliser un mot de passe différent pour chacun des comptes, équipements et accès privés (réseaux sociaux, poste de travail, téléphone mobile, etc.)
- Renouveler en priorité les mots de passe utilisés pendant la mission et sur lesquels pèsent un doute.

9. En cas de doute, faire vérifier les équipements par le Service Informatique du Campus

- Au retour de mission, confier les équipements au Service Informatique du Campus : en cas de saisie de ceux-ci (police aux frontières, accueil d'une organisation, etc.) durant le déplacement et/ou si vous avez des doutes sur l'intégrité de l'un d'eux.

ANNEXE 3

Rappel des textes de loi

OBLIGATION DES FONCTIONNAIRES & ORGANISATION

Loi n° 83-634 du 13 juillet 1983 modifiée portant droit et obligations des fonctionnaires.
Loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat
Décret n°86-83 du 17 janvier 1986 relatif aux dispositions générales applicables aux agents contractuels de l'Etat pris pour l'application de l'article 7 de la loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat.

Arrêté du 6 avril 2009 du MEN et du MESR sur la désignation des Autorités Qualifiées de Sécurité des Systèmes d'Information dans les services d'administration centrale.

Loi n°2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires

LOI n° 2019-828 du 6 août 2019 de transformation de la fonction publique

PROTECTION DES PERSONNES

Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Convention Européenne du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Loi n° 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes (article 226-19 à 24 du Code pénal).

Directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Directive n°95/46/CE, JOCE n° L 281 du 23 novembre 1995).

Recommandations de la CNIL (Commission Nationale Informatique et Libertés) du 28 mars 2001 et du 5 février 2002.

Loi du 21 juin 2004 pour la confiance dans l'économie numérique

Loi n°2004-669 du 9 juillet 2004 (Code pénal et plus particulièrement l'article L432-9 (version du 10 juillet 2004)).

Loi du 6 août 2004 pour la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Décret 2006-358 du 24 mars 2006 relatif à la conservation des communications électroniques.

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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Loi n°2016-1321 du 7 octobre 2016 pour une « République Numérique »

Loi n°2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté

Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles

Ordonnance n°2018-1125 du 12 décembre 2018

Décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

PROTECTION DES LOGICIELS

Ces lois protègent les droits d'auteur, elles interdisent en particulier à l'utilisateur d'un logiciel toute reproduction autre qu'une copie de sauvegarde.

Loi n° 85-660 du 3 juillet 1985 sur la protection des logiciels.

Loi n° 92-597 du 1er juillet 1992 relative au code de la propriété intellectuelle (partie législative).
Loi n° 94-361 du 10 mai 1994 portant mise en œuvre de la directive (C.E.E.) n° 91-250 du Conseil des communautés européennes en date du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur et modifiant le code de la propriété intellectuelle

L'article L 122-5 du code de la propriété intellectuelle n'autorise que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et « les analyses et les courtes citations dans un but d'exemple et d'illustration », toute représentation ou reproduction intégrale ou partielle faite sans consentement de l'auteur est interdite, les citations devront êtres courtes et leur source clairement indiquée.

L'article L122-6-1 du code de la propriété intellectuelle précise les conditions dans lesquelles une personne peut notamment tester le fonctionnement d'un logiciel aux fins d'interopérabilité.

ACCES AUX DOCUMENTS & PROTECTION DES SECRETS PAR NATURE

Loi n° 78-753 du 17 juillet 1978 sur l'accès aux documents administratifs

Loi n°91-646 du 10 juillet 1991 modifiée relative au secret des correspondances émises par la voie des télécommunications (articles 432-9 et 226-15 du nouveau code pénal).

Recommandation N° 901/DCSSI/SCSSI/ du 2 mars 1994 relative à la protection des systèmes d'information traitant des informations sensibles non classifiées de défense.

Instruction générale interministérielle sur la protection du secret de la défense nationale, n°1300/SGDN/PSE/SSD du 25 août 2003.

Ordonnance n°2009-483 du 29 avril 2009

Arrêté du 23 juillet 2010 portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale ;
Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale.

Ordonnance n°2015-1341 du 23 octobre 2015

Loi n°2016-1321 du 7 octobre 2016 pour une « République Numérique » (Code des relations entre le public et l'administration L-300-1 et L-300-2)

ACCES AU RESEAU RENATER

Règles déontologiques d'utilisation du réseau RENATER disponible sur le site Internet de RENATER.

FRAUDE INFORMATIQUE

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique ; cette loi vise à lutter contre la fraude informatique en réprimant :

- les accès ou le maintien frauduleux dans un système d'information
- les atteintes accidentelles ou volontaires au fonctionnement
- la falsification de documents informatiques et leur usage illicite
- la tentative d'accomplissement d'un de ces délits
- l'association ou l'entente en vue de les commettre.

Loi n°2015-912 du 24 juillet 2015 relative aux renseignements
La fraude informatique est définie et sanctionnées par les articles 323-1 à 323-7 du nouveau code pénal dans les termes suivants :

- « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende »

- « Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende »

- « Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. »

RESTRICTIONS A LA LIBERTE D'EXPRESSION

La loi "relative aux infractions de presse" du 29 juillet 1881 modifiée sanctionne notamment la diffamation, le négationnisme, le racisme et les injures.

CONTENUS ILLICITES

LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme

Article 227-23 du Code pénal sur la répression de pédopornographie

ANNEXE 4

Conseils pratiques pour le bon usage de la messagerie

LA MESSAGERIE

Les messages et les paragraphes doivent être courts. Ils doivent être en rapport direct avec le sujet du message.

Traitez un sujet par message et choisissez un titre pertinent pour le champ "objet" de l'en-tête qui apparaît dans la liste des messages du destinataire.

N'utilisez pas le réseau professionnel à des fins commerciales ou pour un travail dont la communauté professionnelle ne peut bénéficier.

Votre signature doit figurer en fin de message. Pour les personnels de l'Établissement, dans le respect de la charte graphique de l'Établissement, elle doit contenir votre nom, votre fonction, votre organisation et votre adresse électronique ainsi que d'autres informations telles que votre numéro de téléphone ou l'adresse postale de votre Campus.

Le bon usage normal de la messagerie implique de respecter quelques règles de bon sens :

- Les personnes en « Copie » n'ont jamais de rôle d'action. Le message est simplement informatif. Seules les personnes « Destinataires » doivent avoir un rôle d'action ;
- Chacun doit veiller à limiter, au strict minimum, le nombre de personne en copie des messages ;
- Lors de la rédaction des messages, n'abusez pas des points d'exclamation, du gras, du souligné ou encore de la couleur rouge ;
- Ne mettez de majuscules que pour souligner un point important ou pour un titre ou un en-tête de paragraphe ;
- Utilisez toujours un vocabulaire posé.

Respectez la voie hiérarchique pour correspondre avec vos supérieurs.

Restez professionnel, poli et respectueux envers la personne avec qui vous communiquez. Il est très facile de retransmettre un courrier électronique en cas de besoin.

Donnez toutes les citations, références et sources d'information et respectez les accords de copyright.

Il est discourtois de retransmettre un message personnel à une liste de diffusion ou à un groupe sans la permission de l'auteur du message.

Maniez l'humour avec prudence. Sans communication directe, vos propos humoristiques peuvent être interprétés comme des critiques ou offenses.

Par précaution, n'envoyez jamais par mail une information que vous n'aimeriez pas voir diffuser publiquement.

Le contenu et la gestion de boîte aux lettres sont sous la responsabilité de l'utilisateur.

Vous devez consulter quotidiennement votre boîte et répondre aux messages qui vous sont adressés.

Il est de votre responsabilité de détruire les messages non importants ou inutiles pour ne pas occuper trop d'espace. Vous devez archiver régulièrement vos messages lus et traités.

ANNEXE 5

Exercice des droits et gestion d'une demande auprès du DPO

Le formulaire de demande d'exercice du droit RGPD est disponible à l'adresse suivante :
https://www.artsetmetiers.fr/rgpd_form