Charte de bon usage du système d'information à l'attention des utilisateurs

L'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte, ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.
Article 1 de la loi du 6 janvier 1978

1. Introduction

La présente charte définit les règles d'usages et de sécurité que l'École Supérieure d'art et Design Grenoble Valence (ESAD GV) et l'utilisateur s'engagent à les respecter: elle précise les droits et devoirs de chacun.
Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

« Un système d'information » peut être défini comme l'ensemble organisé de ressources (personnes, données, procédures, matériels, logiciels, etc.) permettant de traiter, diffuser, mémoriser de l'information en fonction des objectifs d'une organisation.

« Les ressources informatiques » sont les réseaux, les serveurs, les stations de travail, les logiciels, les applications, les bases de données, etc....
C'est une partie du système d'information.

Un « utilisateur » désigne toute personne agissant sur le système d'information

- tout agent titulaire ou non titulaire travaillant pour l'ESAD GV
- tout étudiant inscrit à l'ESAD GV
- tout prestataire ou partenaire ayant contracté avec l'ESAD GV
- toute personne autorisée à accéder à un service numérique de l'ESAD GV

2. Domaines d'application

La présente charte s'applique à tout utilisateur du Système d'Information pour l'exercice de ses activités professionnelles.
L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du système d'information.
La charte est diffusée à l'ensemble des utilisateurs par la messagerie et mise à disposition sur le site Web de l'école dans la brochure.
Elle est systématiquement remise et signée à tout nouvel arrivant par le service Ressources Humaines ou le service de scolarité selon le cas.

Des actions de communication internes sont organisées régulièrement, afin d'informer les utilisateurs des bons usages informatiques.

La présente charte s'applique également aux représentants du personnel et organisation syndicales qui utilisent (cf. charte complémentaire pour les usages syndicaux), dans le cadre de leur mandat, les outils informatiques qui leur sont attribués pour l'exercice de leur activité professionnelle.

3. Conditions d'accès aux systèmes informatiques

L'accès au système d'information (ressources informatiques, service Internet, réseau, ...), est accordé de droit à tout utilisateur dûment inscrit ou employé de la structure. Il est :

- maintenu 6 mois après le départ de l'utilisateur
- ensuite suspendu pour une durée de 6 mois
- ensuite supprimé ainsi que toutes les données laissées par l'utilisateur sur les serveurs de l'ESAD soit un an après la dernière inscription.

Ce droit est personnel et ne peut être cédé même temporairement à un tiers, il est matérialisé par la création d'identifiants nominatifs et confidentiels (couple login / mot de passe).
Dans cette situation l'utilisateur sera responsable des actions effectuées avec ses identifiants.

4. Respect des principes de fonctionnement des systèmes informatiques

Les ressources informatiques mises à votre disposition par l'école sont destinées à être employées dans le cadre de vos études, travail ou recherche et non de divertissement.

Chaque utilisateur est responsable de l'usage qu'il fait du système d'information et des données auquel il accède.
Les utilisateurs ne doivent pas persécuter un individu à l'aide d'outils électroniques.

Il doit être fait un usage raisonnable de toutes les ressources partagées : espace disque, bande passante sur le réseau, occupation des postes de travail, puissance de calcul, logiciels à jetons, etc.

En outre les espaces de stockage réseaux mis à disposition des étudiants n'ont pas vocation à contenir des films, de la musique, et des jeux sauf nécessité pédagogique.

Les utilisateurs signataires de la présente charte s'engagent à respecter les règles ci-dessous.:

- se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques,
- prendre soin du matériel et des locaux informatiques mis à sa disposition
- ne pas déplacer l'équipement informatique et signaler tout dysfonctionnement matériel, logiciel, réseau aux gestionnaires informatiques
- modifier ces équipements et leur fonctionnement, leur paramétrage physique ou logiciel.
- Ne pas mélanger vie privée et vie professionnelle sur les outils professionnels.
- enregistrer les travaux numériques dans les espaces prévus à cet effet (répertoire personnel ou partage). Tout document situé hors de ces répertoires pourra être supprimé sans préalable par les administrateurs du réseau.
- ne pas utiliser les ressources de l'école pour tenir des propos (oraux ou écrits) qui constituent des infractions au sens de la loi du 29 juillet 1881 sur la liberté de la presse, notamment des propos à caractère insultants, injurieux, diffamatoires, racistes, pornographiques, pédophiles ou attentatoires au respect d'autrui.
  L'utilisateur est fermement encouragé à respecter les règles de politesse d'usage. Ces règles sont applicables quel que soit le média ou la technologie utilisé (forums, messagerie électronique, dialogue en direct, ...), et quel que soit le destinataire (enseignant, personnel, étudiant)
- ne pas porter atteinte à l'intégrité d'autres sites ou systèmes qu'ils soient ou non connectés au réseau,
- ne pas tenter d'accéder à des ressources du Système d'Information et aux communications entre tiers, pour lesquelles il n'a pas reçu d'habilitation explicite, notamment en :
  - usurpant l'identité d'une autre personne,
  - s'appropriant le mot de passe d'un autre utilisateur,
  - se connectant sur un site en accès limité sans y être autorisé,
  - dissimulant sa véritable identité,
  - accédant modifiant ou supprimant à des informations appartenant à d'autres utilisateurs du réseau sans autorisation,

- ne pas rendre accessibles à des tiers les services qui lui sont offerts dans le cadre de son travail, en particulier les moyens d'accès et d'identification (tels que les adresses électroniques, badges, codes et mots de passe) qui sont personnels et ne doivent en aucun cas être cédés,
- ne pas nuire volontairement au bon fonctionnement du Système d'Information et des réseaux ou à l'activité d'un tiers par des manipulations anormales des matériels ou par l'introduction volontaire de logiciels malveillants (virus, chevaux de Troie,..)
- ne pas connecter directement aux réseaux locaux des matériels n'appartenant pas à l'école sans prévenir au préalable les personnes en charge du réseau,
- 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,
- ne pas développer, installer ou copier un programme pour contourner la sécurité ou saturer les ressources informatiques,
- ne pas introduire d'outils d'intrusion et effectuer des tests de sécurité sur le Système d'Information sans autorisation préalable.
- ne pas utiliser les ressources mise à sa disposition pour un usage commercial à titre privé

Toute utilisation d'outils ou services externes qui conduisent à faire transiter ou à déposer des informations professionnelles et/ou pédagogiques hors des supports et des services mis en œuvre par l'ESAD engage la responsabilité de celui qui les utilise.
En effet, ces pratiques présentent un risque de vulnérabilité particulier du point de vue, d'une part, de la confidentialité des données, d'autre part de la protection du patrimoine scientifique, technique et littéraire mais également des libertés individuelles.

5. Internet

L'ESAD est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées (en volume).

Une utilisation ponctuelle pendant les périodes de pause, pour un motif personnel, les sites internet et des réseaux sociaux dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l'institution, est tolérée.
Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution.

Les utilisateurs s'engagent à ne pas utiliser l'accès à internet 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, telle que des textes, images, photographies, œuvres musicales, œuvres audiovisuelles, logiciels et jeux vidéo, sans autorisation.
Ces manquements sont réprimés par l'article L335-2 du code de la propriété intellectuelle qui prévoit des peines pouvant aller jusqu'à 5 ans d'emprisonnement et 500 000 euros d'amende.

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

Merci également de :

- limitez l'usage des lecteurs en streaming de média (film, musique…) à un usage pédagogique et/ou professionnel (Youtube, Deezer, Spotify …)
- optimisez vos images, sons et autres documents avant de les envoyer via internet.
- ne pas utiliser des logiciels de P2P (hors usage pédagogique) ou d'autres logiciels pouvant affaiblir la sécurité des systèmes informatiques de l'école.

6. Messagerie électronique

a. Conditions d'utilisation

L'ESAD GV s'engage à mettre à la disposition de l'utilisateur une boîte à lettres institutionnelle nominative lui permettant d''émettre et de recevoir des messages électroniques.
L'usage des adresses institutionnelles de type prenom.nom@esad-gv.fr doit être privilégié dans tout échange pédagogique.
L''utilisation de cette adresse nominative est de la responsabilité de l'utilisateur.

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel (Objet du message « Personnel : ») bénéficiera du droit au respect de la vie privée et du secret des correspondances. À défaut, le message est présumé professionnel. L'ESAD s'interdit d'accéder aux dossiers et aux messages identifiés comme « personnel » dans l'objet de la messagerie de l'agent

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'établissement.

L'utilisation de la messagerie est interdite pour toute propagande à caractère politique, religieux ou philosophique.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par le service informatique en termes de volumétrie et de taille maximale d'envoi/réception d'un message et de la gestion de l'archivage de la messagerie

b. Confidentialité et réserve

Les règles habituelles en matière de communication écrite s'appliquent pleinement à la messagerie. Si un message électronique peut paraître comme « suspect », il n'en demeure pas moins qu'il est porteur d'information et que sa présentation sous forme électronique le rend très facilement imprimable, reproductible à de nombreux exemplaires, transmissible, et diffusable à un nombre conséquent de correspondants.
Les niveaux de confidentialité de l'information et les modalités de traitement en fonction du niveau de discrétion en usage dans la collectivité sont totalement applicables aux courriels.
Les règles d'éthique et de secret professionnel, de déontologie, d'obligation de réserve et de devoir de discrétion imposés notamment par l'article 26 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, et en usage dans les différents métiers exercés dans la collectivité, sont aussi totalement applicables.
À cet égard, il est important de rappeler que la révélation d'une information à caractère secret par une personne qui en est dépositaire est punie par l'article 226-13 du Code pénal d'un an d'emprisonnement et de 15 000 euros d'amende.

c. Comportements/actes illicites

Le Code pénal interdit aux utilisateurs de la messagerie tout stockage, transit et diffusion de documents proscrits par la loi.
C'est notamment le cas des images et/ou textes pédophiles (article 227.23 et suivants du Code pénal) et/ou racistes (article 225-1 et suivants du Code pénal) et/ou le trafic de stupéfiants (article 222-34 et suivants du Code pénal) et/ou les atteintes à la Sécurité Sociale (article 410-1 et suivants du Code pénal).

Certes, un agent ne peut être tenu pour responsable s'il reçoit, à son insu, de tels documents, mais il lui est imposé de les détruire.
De même, il doit s'abstenir de tout comportement pouvant induire les tiers à lui adresser de tels documents. Ainsi, il devra s'abstenir de participer à des forums ou d'accéder à des sites pouvant traiter de sujets racistes, pornographiques ou pédophiles.
En effet, les administrateurs de ce genre de sites risquent d'enregistrer son adresse et de l'inclure ensuite dans des courriels de masse comportant des pièces jointes illicites. Au cas exceptionnel, où une telle situation se serait produite fortuitement, il y a obligation d'informer son supérieur hiérarchique et la DCSI qui trouvera la parade appropriée.
Les utilisateurs qui auraient l'illusion que leurs manquements seraient indécelables doivent savoir que des moyens techniques de traçabilité existent.

d. Consultation de la messagerie pour nécessité de service

En cas d'absence d'un agent et afin de ne pas interrompre le fonctionnement du service, la service informatique peut, ponctuellement transmettre au supérieur hiérarchique un message électronique professionnel.
Le supérieur hiérarchique n'a pas accès aux autres messages de l'agent. L'agent concerné est informé dès que possible de la liste des messages qui ont été transférés.
En cas d'absence prolongée d'un agent (longue maladie), le chef de service peut demander au service informatique, après accord de son direction, la mise en place d'un message d'absence indiquant la
démarche à suivre.

7. Équipements

a. Nomades

On entend par « équipements nomades » tous les équipements techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD-ROM, clef USB, etc.) mis à disposition par l'école.
L'agent bénéficiant d'un ou plusieurs de ces équipements en est responsable. En cas de dégradation, perte, vol sa responsabilité peut être engagée.
Lorsqu'un agent dispose d'un ordinateur portable et s'absente de son bureau, il doit attacher physiquement l'ordinateur à l'aide de l'antivol si celui-ci est présent ou fermer son bureau.
L'utilisation de smartphones professionnels pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en

cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

b. Matériel de prêt

L'utilisateur est responsable des équipements qui lui sont remis et de son usage dès sa prise en charge et jusqu'à sa restitution, et ne doit pas contourner la politique de sécurité mise en place.
L'utilisateur doit informer immédiatement le gestionnaire en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte et blocage distant.

c. Équipements personnels

On entend par « équipements personnels » tous équipements non fournis par l'école et qui appartient personnellement à l'agent.
Ces équipements ne peuvent être connectés au réseau informatique de la collectivité sans l'accord du service informatique.
Seule l'utilisation de la messagerie professionnelle sur les équipements personnels est tolérée sur le réseau de l'école.
L'utilisateur se doit de sécuriser ses équipements personnels pour éviter toute intrusion malveillante (anti-virus, anti-spam, anti-malware, ...).
L'utilisation de clef USB et disque dur externe personnels est tolérée. Ceux-ci devront être soumis à un scan antivirus à l'aide de celui installé sur les postes de travail avant toute utilisation.

8. Téléphone

L'ESAD met à disposition de certains utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.
L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable et exceptionnelle.
Des restrictions d'utilisation par les agents des téléphones fixes sont mises en place en tenant compte de leurs missions. À titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

Toutefois, en cas d'utilisation manifestement anormale, le service informatique se réserve le droit d'accéder aux numéros complets des relevés individuels.

9. Moyens d'impression

Les moyens d'impression comme les copieurs, gérés par le service informatique, possèdent un système de comptabilisation des volumes imprimés, des copies.
Ils sont destinés à un usage exclusivement professionnel ou pédagogique
Le service informatique dans le cadre de la bonne gestion peut accéder à ces données.

10. Respect de la propriété intellectuelle

L'utilisation des ressources informatiques implique le respect des droits de propriété intellectuelle de l'ESAD GV ainsi que ceux de ses partenaires et, plus généralement, de tous tiers titulaires de tels droits.

Chaque utilisateur se doit :

- d'utiliser les logiciels dans les conditions des licences souscrites,
- de ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies, sons, vidéos ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits,
- de respecter le droit des marques.

L'étudiant est informé que ses réalisations et/ou travaux universitaires dans le cadre de sa formation, mémoire, thèse, ... peuvent faire l'objet d'un contrôle anti-plagiat par tout moyen, notamment par l'usage d'applications et/ou logiciels spécifiques.

11. Règles de sécurité

L'ESAD GV met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.
Les identifiants fournis à chaque utilisateur constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive.

Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité générale du Système d'Information, il doit :

• appliquer et respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe :

- il doit : choisir un mot de passe non trivial composé de lettres majuscules et minuscules, de chiffres et de caractères spéciaux afin d'être difficilement devinable,
- garder strictement confidentiels son (ou ses) identifiants et ne pas le(s) dévoiler à un tiers,
- modifier son mot de passe en cas de doute. En cas de compromission manifeste du mot de passe, l'ESAD se réserve le droit de suspendre temporairement le compte jusqu'au règlement du problème rencontré,
- ne pas quitter son poste de travail (ni ceux en libre-service) en laissant des ressources ou services accessibles et penser à se déconnecter ou à verrouiller la session,
- utiliser des mots de passe différents pour accéder à des environnements différents (sites universitaires, sites commerciaux, réseaux sociaux, etc.) modifier ses mots de passe à minima une fois par an,
- assurer la protection des informations sensibles (pour lesquelles a été identifié un besoin direct ou indirect de confidentialité) :
  o protéger ses données en effectuant régulièrement des sauvegardes,
    - protéger ses fichiers et données contre la lecture et l'écriture en utilisant tous les moyens mis à leur disposition par le système d'exploitation utilisé,
    - éviter de les transporter sans protection sur des supports non fiabilisés (clés USB, ordinateurs portables, disques externes, etc.) ne pas les déposer sur un serveur externe et/ou ouvert au grand public,
- avertir par mail (informatique@esad-gv.fr) dans les meilleurs délais de tout dysfonctionnement constaté ou de découverte d'anomalies affectant la sécurité du Système d'Information, tel un accès frauduleux et notamment l'utilisation illicite de son propre compte.

12. Télétravail

a. Sécurisez votre connexion internet

Assurez-vous du bon paramétrage de votre box Internet. Vérifiez son mot de passe d'accès administrateur, changez-le s'il est faible et mettez à jour son logiciel interne. Le site web de

votre opérateur (par exemple celui de Bouygues, SFR, Orange et Free), vous accompagnera dans la bonne mise en œuvre de ces étapes.
Si vous utilisez le Wi-Fi, activez l'option de chiffrement WPA2 ou WPA3 avec un mot de passe long et complexe (l'Agence nationale de la sécurité des systèmes d'information (ANSSI) recommande par exemple une vingtaine de caractères). Désactivez la fonction WPS et supprimez le Wi-Fi invité.
Ne vous connectez qu'à des réseaux de confiance et évitez les accès partagés avec des tiers.

b. Equipements

- Favorisez l'usage d'équipements fournis et contrôlés par votre entreprise
  Si vous en avez la possibilité, utilisez autant que possible le VPN (Virtual Private Network ou réseau privé virtuel) ou la connexion RDS mise à disposition par votre établissement : privilégiez l'échange de données à travers les stockages disponibles depuis le VPN plutôt que par la messagerie électronique;
  connectez-vous au moins une fois par jour au VPN pour appliquer les mises à jour;
  désactivez votre VPN seulement lorsque vous utilisez des services consommateurs de bande passante, comme le streaming vidéo, qui ne nécessitent pas de passer par le réseau de votre entreprise.

- Si vous devez utiliser un ordinateur personnel, assurez-vous qu'il est suffisamment sécurisé
  Cela doit passer par:
  l'installation d'un antivirus et d'un pare-feu. Si vous êtes sur le système d'exploitation Windows 10, vérifiez l'état de vos systèmes de protection au moyen du centre de sécurité ;
  l'utilisation d'un compte personnel avec des droits limités, protégé par un mot de passe fort et non partagé avec d'autres personnes (par exemple avec d'autres membres de votre famille) et sur lequel les applications installées se limitent au strict nécessaire ;
  la mise à jour régulière du système d'exploitation et des logiciels utilisés, notamment le navigateur web et ses extensions. Supprimez ou passez au plus vite à une version récente des logiciels dont le support ou la mise à jour sont abandonnés, comme le système d'exploitation Windows 7 (et les versions antérieures comme Windows XP) dont le support n'est plus assuré depuis le 14 janvier 2020 ou les versions de MacOsX qui ne

durent que 4 ans en moyenne;
des sauvegardes régulières de votre travail de préférence sur les infrastructures de l'école;

c. Mot de passe

L'utilisation de mots de passe forts sur l'ensemble de vos services et l'activation de l'authentification à deux facteurs (clef d'authentification, jeton, SMS) dès que cela est proposé par le service. Les gestionnaires de mots de passe, par exemple les logiciels KeePass ou ZenyPass, vous permettront de sécuriser leur stockage et leur gestion.
La CNIL propose un outil pour créer rapidement des mots de passe robustes ainsi qu'un tutoriel pour utiliser le gestionnaire de mots de passe Keepass.

d. Téléphones

Si vos téléphones ne sont pas gérés par la structure ou que la structure ne dispose pas d'outils de gestion de ces matériels faîtes particulièrement attention aux points suivants :
Parce qu'ils vous accompagnent partout, les téléphones portables sont particulièrement exposées à la perte et aux vols:
Évitez d'y enregistrer des informations confidentielles: codes secrets, codes d'accès, coordonnées bancaires, etc ;
Activez le code PIN et mettez en place un délai de verrouillage automatique du téléphone. Évitez les codes trop faciles (date de naissance, 0123, etc.) ;
Activez le chiffrement des informations sur votre téléphone lorsque c'est possible;
Notez le numéro « IMEI » du téléphone pour le bloquer en cas de perte ou de vol ;
N'installez des logiciels que depuis les plateformes officielles et évitez à tout prix les applications de sources inconnues ;
Lorsque vous installez de nouvelles applications sur votre appareil, lisez les conditions d'utilisation et la politique de confidentialité et limitez les données auxquelles elles peuvent avoir accès au strict nécessaire ;
Réglez les paramètres de géolocalisation afin de toujours contrôler quand et par qui être géo-localisé.

e. Communiquez en toute sécurité

Évitez de transmettre des données confidentielles via des services grand public de stockage, de partage de fichiers en ligne, d'édition collaborative ou via des messageries. À défaut,

chiffrez les données avant de les transmettre et transmettez les clés de chiffrement via un canal de communication distinct (par exemple, communication du mot de passe par téléphone ou SMS). Des logiciels grand public comme 7-zip et Zed! permettent de chiffrer les données avec des algorithmes réputés fiables.
Installez uniquement des applications autorisées par votre entreprise. Si votre entreprise ne propose pas de système de déploiement d'application,
téléchargez celles-ci depuis les sites ou les magasins officiels des éditeurs.
Privilégiez des outils de communication chiffrés de bout en bout, si votre entreprise ne vous fournit pas d'outils de communication sécurisés.
Évitez les applications gratuites qui ne vous offrent pas de garanties fortes de sécurité.
Dans tous les cas, respectez toujours les instructions de votre
employeur.
Privilégiez les systèmes de visioconférence qui protègent la vie privée. Vérifiez les conditions d'utilisation de votre logiciel pour vous assurer que ces outils garantissent la confidentialité de vos données et ne les réutilisent pas pour d'autres finalités.

f. Hameçonnage

Soyez particulièrement vigilant sur les tentatives d'hameçonnage
Les pirates profitent des périodes de crise ou de trouble pour inventer de nouvelles escroqueries et tirer profit de ces événements. Soyez vigilant à tout contact :
de personnes que vous ne connaissez pas, surtout si elles vous invitent à cliquer sur des liens ou à ouvrir un fichier;
d'une personne connue vous envoyant une communication inhabituelle. Essayez de vérifier cette information par un autre canal (téléphone, SMS, mail);
de personnes cherchant à créer un sentiment d'urgence ou de danger. Le cas échéant, toujours utiliser un autre canal pour vérifier les informations communiquées, par exemple en effectuant une recherche sur Internet.
En cas de doute, demandez de l'aide à votre Responsable des systèmes d'information pour vous accompagner dans le choix d'une solution qui convient à votre besoin.

13. Responsabilités - Limitation des usages et sanctions des abus

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte peut entrainer une limitation ou un blocage de son accès au système d'information.

Il est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre. :

- Dans un premier temps, en un rappel à l'ordre émanant du service informatique, après avis de la direction générale, en cas de non-respect des règles énoncées par la charte
- Dans un second temps, et en cas de renouvellement, après avis de la direction générale, du supérieur hiérarchique de l'agent ou du conseil pédagogique selon le cas, en des sanctions disciplinaires adoptées après saisine du conseil de discipline.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information (cf. liste des textes en annexe) est susceptible de sanctions pénales prévues par la loi.

14. Entrée en vigueur de la charte

La présente charte a été adoptée après information et avis du comité technique.
Elle est applicable à compter du 01/10/2021.

15. Rappels juridiques

L'ESAD GV se réserve le droit d'engager des poursuites au niveau pénal indépendamment des sanctions administratives vis-à-vis de toute personne ayant directement ou indirectement participé à la violation de la présente charte.

16. Respect des dispositions légales sur la protection des données personnelles

Conformément au Règlement général sur la protection des données (RGPD – 2016/679) et à la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles :

- 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.

- Les traitements de données à caractère personnel consistent en toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte,
  enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...).
- Tous les traitements de données à caractère personnel sont soumis aux obligations et formalités préalables prévues par la législation sur la protection des données.
  Afin d'appliquer les mesures nécessaires au respect des dispositions légales, tout utilisateur souhaitant procéder à un traitement de données devra en informer, dès la phase de conception, le délégué à la protection des données (DPO) à cette adresse : dpo-contact@esad-gv.fr,
  Par ailleurs, conformément aux dispositions légales, chaque personne concernée par un traitement dispose des droits d'accès, de rectification, de limitation et de portabilité relatifs à l'ensemble des données la concernant, y compris les données portant sur l'utilisation des systèmes d'information. Dans certains cas, les droits d'opposition et d'effacement peuvent également s'exercer.
  L'utilisateur est tenu de respecter l'application de ces droits conformément aux dispositions légales.
  Chaque personne concernée par un traitement de ses données personnelles peut demander l'exercice de ces droits, notamment en contactant le délégué à la protection des données (DPO).