

 <p>ESTP PARIS L'ÉCOLE DES GRANDS PROJETS</p>	Annexe 1 au Règlement Intérieur de la formation initiale	FO-001-MSI-XX-001-V1
	Charte de bon usage des moyens informatiques de l'ESTP Paris	30/06/2022
	<i>A l'attention des élèves FISE, FISA et stagiaires Formation Continue de l'ESTP Paris</i>	Page 1/5

VERSION	DATE	REDACTEUR	VERIFICATEUR	APPROBATEUR
N°1	20/06/2022	Hervé Guillermet Directeur des Systèmes d'Information	Serge Le Strat Directeur de l'Enseignement Antoine Paquereau Responsable juridique	Rachel Fracz-Vitani Secrétaire Générale

Avertissement liminaire :

L'utilisation des services informatiques mis à disposition par l'ESTP vaut acceptation de la présente charte définissant les règles d'usage et de sécurité du Système d'Information (SI) que l'ESTP met à disposition de ses Apprenants.

ESTP offre à ses Apprenants différents services comme le courriel, le stockage de données, le wifi, l'accès à internet, l'accès à ses plateformes et à son cloud, la mise à disposition des applications standards et métiers des salles et laboratoires d'enseignement ou encore le portail web et les impressions. Tous ces services sont à considérer comme des outils de travail.

Les droits d'accès aux moyens informatiques sont octroyés après l'engagement de respecter la présente.

Conséquences d'un comportement indésirable :

Un comportement contraire aux présentes règles peut mener à des sanctions allant de la réprimande à la suspension des droits d'accès au Système d'Information. Dans les cas jugés particulièrement graves, selon l'article 13 du Règlement Intérieur de la formation initiale, cela peut mener à une exclusion.

Article 1 : Conditions d'utilisation

Tout Apprenant au sein de l'ESTP est responsable de ce qui est réalisé sous son nom d'utilisateur, de l'utilisation qu'il fait des ressources informatiques, de l'Internet et du wifi. Il s'engage à n'effectuer aucune opération susceptible de porter atteinte de quelque façon que ce soit :

- A l'intégrité, la sécurité, la disponibilité du Système d'Information de l'ESTP ;
- A l'image de l'ESTP ;
- Au respect de la vie privée, au droit à l'image, au droit d'auteurs ;
- A l'ordre et la sécurité physique ;
- Au respect des lois et règlements en vigueur.

La sécurité informatique consiste, d'une part, à assurer la confidentialité et l'intégrité des données et, d'autre part, à garantir l'exploitation des services offerts.

 <p>ESTP PARIS L'ÉCOLE DES GRANDS PROJETS</p>	Annexe 1 au Règlement Intérieur de la formation initiale	FO-001-MSI-XX-001-V1
	Charte de bon usage des moyens informatiques de l'ESTP Paris	30/06/2022
	<i>A l'attention des élèves FISE, FISA et stagiaires Formation Continue de l'ESTP Paris</i>	Page 2/5

Il est strictement interdit à tout Apprenant de l'ESTP :

- De mettre en œuvre des services d'accès externes (modems ou autres moyens de télécommunications directs) sur votre poste de travail ou les matériels de l'ESTP ;
- De créer des réseaux informatiques, des serveurs internet, de messagerie, de jeux, de réseau social ou autres types de réseau sur le réseau ESTP ;
- De permettre l'accès au réseau ESTP à des tiers au travers d'un PC connecté ;
- De capturer le trafic du réseau de l'ESTP ;
- De rediriger le trafic ;
- D'attaquer le réseau ;
- De s'allouer des adresses IP¹ sans autorisation ;
- D'accéder à des informations privées concernant d'autres utilisateurs du réseau ;
- De modifier ou détruire des informations sur un des systèmes connectés au réseau ;
- D'interrompre le fonctionnement normal du réseau ;
- De masquer sa propre identité.

Article 2 : Règles de bon usage des moyens informatiques

L'Apprenant s'engage à :

- Ne jamais utiliser de clé USB sans la passer au préalable sous antivirus ;
- Ne jamais communiquer son mot de passe ;
- Ne pas laisser son poste de travail sans surveillance ; lors d'une absence même brève (pause), verrouiller le poste ;
- Avant de quitter la salle informatique, arrêter tous ses travaux, fermer sa session et éteindre le PC ;
- Ne jamais tenter de s'introduire dans un système ou un environnement informatique sans avoir, au préalable, reçu une autorisation d'accès de la Direction des Systèmes d'Information ;
- Eviter de monopoliser les imprimantes aux heures d'affluence avec de longs documents tels que rapport de stage, projet, ... Les imprimantes ne sont pas des photocopieuses ;
- Respecter le quota d'impression attribué en début d'année pour utiliser le parc imprimante et traceur ;
- Prévenir le support informatique et, si nécessaire, la Direction de tout incident, même bénin, et en particulier ceux liés à la sécurité et à la confidentialité des données ;
- S'assurer qu'un logiciel antivirus à jour est sur son poste de travail ;
- Sauvegarder régulièrement son travail ;
- Respecter le planning de maintenance informatique affiché dans les salles informatiques.

ESTP effectuera une maintenance évolutive et corrective des ressources mises en œuvre.

¹ Internet Protocol

 <p>ESTP PARIS L'ÉCOLE DES GRANDS PROJETS</p>	Annexe 1 au Règlement Intérieur de la formation initiale	FO-001-MSI-XX-001-V1
	Charte de bon usage des moyens informatiques de l'ESTP Paris	30/06/2022
	<i>A l'attention des élèves FISE, FISA et stagiaires Formation Continue de l'ESTP Paris</i>	Page 3/5

Article 3 : Utilisation d'internet, du wifi et de la messagerie

L'ESTP a mis en place des mesures techniques, conformément à la législation en vigueur, qui permettent de répondre aux impératifs de sécurité. Internet est un outil de travail ouvert à des usages pédagogiques et de recherches scientifiques.

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

Pour protéger efficacement l'accès à internet, il est strictement interdit :

- D'accéder à un site internet inapproprié dans le cadre pédagogique ;
- D'accéder à un site internet illégal au regard de la loi française ou contraire aux bonnes mœurs ;
- De télécharger des jeux, logiciels malveillants ou illicites, de sons, vidéos, images ;
- D'utiliser abusivement (en volume et temps passé) l'accès internet à des fins privées ;
- De publier sur les sites internet et portails de l'ESTP ;
- D'accéder à des sites, chat et forums malveillants ;
- D'utiliser le logo ou l'image ESTP sur des supports informatiques (sites, forums, newsletter...) sans son accord au préalable.

Article 4 : Accès aux salles et laboratoires d'enseignement

L'ESTP met à disposition des ressources informatiques dans les salles et laboratoires d'enseignement, afin que les Apprenants puissent travailler sur les logiciels à vocation pédagogique et en libre-service.

L'ESTP offre aussi offre un catalogue de services :

- Portails web et messagerie accessibles depuis l'extérieur ;
- Espaces partagés ;
- Applications standard et métiers (office, matlab, autocad, ansys, ls-dyna, revit, civil 3D, ...) ;
- Outils de communication (messagerie, visio-conférence, tchat) ;
- Impression.

Chaque Apprenant est tenu pour responsable pour toute utilisation de ces moyens informatiques et doit respecter les consignes suivantes. Il est strictement interdit :

- De modifier ou débrancher le câblage des pc et imprimantes ;
- De changer, installer ou utiliser des jeux, des logiciels illégaux, des logiciels ou des images et vidéos qui ne sont pas en rapport avec l'enseignement ;
- D'introduire délibérément des virus ou d'autres logiciels dangereux ;
- De copier des logiciels protégés par des droits d'auteurs ;
- De désinstaller ou supprimer les logiciels ;
- De modifier la configuration du PC ;
- D'installer les logiciels sans détenir de licences nécessaires.

 <p>ESTP PARIS L'ÉCOLE DES GRANDS PROJETS</p>	Annexe 1 au Règlement Intérieur de la formation initiale	FO-001-MSI-XX-001-V1
	<p align="center">Charte de bon usage des moyens informatiques de l'ESTP Paris</p> <p align="center"><i>A l'attention des élèves FISE, FISA et stagiaires Formation Continue de l'ESTP Paris</i></p>	30/06/2022
		Page 4/5

Article 5 : Utilisation des terminaux personnels (ordinateur portable, tablette, smartphone)

L'ESTP accepte l'introduction des terminaux personnels. Ceux-ci doivent répondre aux enjeux importants de sécurité et confidentialité exigés par l'ESTP :

L'Apprenant doit disposer d'un antivirus à jour et des derniers patches de sécurité à jour, avant de connecter son matériel personnel sur le réseau ESTP ;

L'Apprenant est responsable de la criticité des informations échangées ;

L'Apprenant assurera lui-même la protection de son matériel ;

L'Apprenant est seul responsable de son matériel. Si celui-ci est volé, perdu ou cassé, l'ESTP n'assurera pas le support informatique des matériels, ni son remplacement ;

L'ESTP n'est, en aucun cas, responsable du matériel personnel (ordinateur portable, tablette et smartphone) de l'Apprenant, ni du contenu des données.

Article 6 : Sanctions

Tout Apprenant n'ayant pas respecté les règles de bon usage des ressources informatiques énoncées dans la présente Charte s'expose à des sanctions disciplinaires de la part de l'ESTP ou à des poursuites pénales suivant le cas, tel que ceci est exposé dans le Règlement Intérieur.

 <p>ESTP PARIS L'ÉCOLE DES GRANDS PROJETS</p>	Annexe 1 au Règlement Intérieur de la formation initiale	FO-001-MSI-XX-001-V1
	Charte de bon usage des moyens informatiques de l'ESTP Paris <i>A l'attention des élèves FISE, FISA et stagiaires Formation Continue de l'ESTP Paris</i>	30/06/2022
		Page 5/5

Annexe : Principales références législatives et réglementaires :

- Loi du 29 juillet 1881 modifiée relative à la liberté de la presse (notamment chapitre IV : Des crimes et délits commis par la voie de la presse ou par tout autre moyen de publication).
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- (cf. articles 226-16 à 226-24 et R625-10 à R625-13 du Code pénal).
- Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dite "loi Godfrain" (cf. articles 323-1 à 323-7 du Code pénal).
- Code pénal, notamment les articles 226-1 et suivants relatifs à l'atteinte à l'intimité de la vie privée, les articles 226-15 et suivants relatifs au secret des correspondances, l'article 227-23 relatif à la détention et/ou la diffusion de documents à caractère pédophiles et l'article 227-24 relatif à la diffusion et/ou au commerce de messages à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine.
- Jurisprudence et Code civil, notamment les articles relatifs au droit à l'image et à la protection de la vie privée.
- Loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle telle que modifiée jusqu'à l'ordonnance n° 2009-901 du 24 juillet 2009.
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et le décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.
- Loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique.
- Création de l'Arcom depuis le 1^{er} janvier 2022 : **Autorité de régulation de la communication audiovisuelle et numérique**, née de la fusion du Conseil supérieur de l'audiovisuel (CSA) et de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi).
- Loi n°2006-961 du 1^{er} août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information.
- Règlement européen 2019/881 dit « Cybersecurity Act ».