Charte de bon usage du Système d'Information (SI) de l'Institut Lemonnier

Les droits d'accès aux ressources informatiques de l'Institut Lemonnier ne sont octroyés qu'après l'engagement de respecter la présente charte et pourront être suspendus ou retirés dès lors que l'utilisateur dérogera à ces obligations ou enfreindra la loi.

Le Système d'Information est composé de l'ensemble des moyens matériels, logiciels, applications, base de données et réseaux de télécommunication, pouvant être mis à disposition par l'Institut Lemonnier. Le terme « utilisateur » désigne tout élève, étudiant, stagiaire ou résident ayant accès aux ressources du SI.

Conditions d'utilisation

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques et 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 SI de l'Institut Lemonnier
- A l'image de l'Institut Lemonnier
- Au respect de la vie privée, au droit à l'image, au droit d'auteur et droits voisins de toute personne physique ou morale, privée ou publique.
- Aux biens et personnes par des faits constituants des infractions pénales.

Accès au Système d'information :

L'utilisation des ressources informatiques de l'Institut Lemonnier, qui suppose l'approbation de la présente charte, est soumise à autorisation préalable d'un membre de la communauté éducative. Elle peut être retirée, partiellement ou totalement, temporairement ou définitivement, en cas de non respect de la charte.
Le droit d'accès aux ressources informatiques est **personnel** et **incessible**. Il disparait dès que son utilisateur ne remplit plus les conditions qui lui ont autorisé l'accès.

Espace de stockage :

Chaque utilisateur possède un espace de stockage réservé exclusivement aux données pédagogiques. Dans ce cadre, les membres de la communauté éducative ont un droit d'accès à cet espace.
L'utilisation de matériel informatique personnel (clé USB, lecteur MP3…) est toujours soumise à autorisation.

Tablettes en location :

Les élèves bénéficiant d'une tablette, mise à leur disposition dans le cadre d'une convention de location-vente, s'engagent à être en permanence en possession de celle-ci sur le temps des cours, et à l'utiliser uniquement pour l'activité pédagogique décidée par l'enseignant.
Durant la période du contrat de location, les membres de la communauté éducative ont un droit d'accès aux données situées sur la tablette et l'ensemble des règles de sécurité définies au sein de la charte informatique est appliqué. En particulier, l'élève s'engage à ne pas désinstaller les logiciels mis en place par l'établissement pour la gestion des tablettes à l'institut Lemonnier.

Conformités aux lois et règlements :

L'utilisateur s'engage à un usage du SI de l'Institut Lemonnier conforme aux lois et règlements en vigueur :

- Propriété intellectuelle : utilisation des logiciels et des données dans les conditions des licences souscrites. Ne pas télécharger, reproduire, copier, diffuser, modifier ou utiliser tout document numérique protégé par le droit d'auteur ou un droit voisin, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits. Respect du droit des marques.
- Diffusion de l'information : sont interdits les messages diffamatoires, discriminatoires ou injurieux, les provocations et apologies (crime, racisme, négationnisme, crime de guerre, …) l'accès, la détention, la diffusion d'image à caractère pédophile ou pornographique, la

publication d'informations confidentielles sans autorisation préalable.
- Droit à la vie privée : le droit de l'image et le droit de représentation impliquent qu'aucune image ou information relative à la vie privée d'autrui ne doit être mise en ligne sans l'autorisation de la personne intéressée.

Usage privé réservé uniquement pour la résidence étudiante et l'internat.

L'utilisation à titre privé du SI est tolérée sous réserve qu'elle soit éthique, licite, non lucrative, et raisonnable en termes de fréquence et de durée.

Règles de sécurité applicables

Conformément à la politique de sécurité de l'Institut Lemonnier, la protection des ressources mises à disposition de l'utilisateur nécessite l'application de quelques règles élémentaires :

- Respecter la gestion des accès, en particulier ne pas utiliser les mots de passe d'un autre utilisateur, ni chercher à les connaitre
- Conserver son mot de passe de façon strictement confidentielle et le changer en cas de doute (voir le responsable du SI).
- Ne pas tenter d'accéder à des ressources du SI, à des informations détenues par d'autres utilisateurs ou aux communications entre tiers, pour lesquelles il n'y a pas d'autorisation explicite. A noter que la capacité d'accéder à une information n'implique pas que l'accès soit effectivement autorisé.
- Ne pas rendre accessible à des tiers les services qui lui sont offerts par l'Institut Lemonnier.
- Se conformer aux dispositifs et recommandations standards pour lutter contre les virus et attaques informatiques (Antivirus installé, fonctionnel et à jour).
- Signaler aux responsables toute anomalie ou dysfonctionnement des systèmes informatiques, notamment tout ce qui concerne la sécurité du SI.
- Ne pas nuire volontairement au bon fonctionnement des ressources informatiques et des réseaux par des manipulations anormales du matériel ou par l'introduction de logiciels malveillants.
- **Ne pas quitter son poste de travail sans se déconnecter.**

Contrôles

Des contrôles techniques peuvent être effectués :

- **Dans un souci de protection des élèves et notamment des mineurs ;**

L'Etablissement se réserve la possibilité de procéder à un contrôle des sites visités par les élèves afin d'éviter l'accès par ces derniers à des sites illicites ou requérant l'âge de la majorité, notamment par lecture des journaux d'activité du service d'accès au réseau.

- **Dans un souci de sécurité du réseau et/ou des ressources informatiques ;**

Pour des nécessités de maintenance et de gestion technique, l'utilisation des services et notamment des ressources matérielles et logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment dans le respect des règles relatives à la protection de la vie privée et au respect des communications privées. L'Etablissement se réserve, dans ce cadre, le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système.

- **Dans un souci de vérification que l'utilisation des services reste conforme aux objectifs pédagogiques**

Sanctions et abus

En cas de non-respect des règles définies dans la présente charte, l'Institut Lemonnier pourra prendre toute mesure utile à la préservation de ses intérêts et des intérêts des personnels, usagers, partenaires publics ou privés ou tiers, notamment :

- Limiter ou interdire l'accès au SI de l'Institut Lemonnier.
- Appliquer des sanctions disciplinaires prévues dans le code de vie de l'Institut Lemonnier.

L'Institut Lemonnier est également tenu de signaler aux représentants de la loi toute violation de la législation constatée.

Annexe : Principales références législatives et réglementaires :

La législation relative à la protection des systèmes informatiques notamment les articles 323-1 à 323-7 du Code Pénal :
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 30000 euros 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 45000 euros d'amende ;

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ;
Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ;
La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines. Les personnes physiques coupables des délits prévus au présent chapitre encourent également des peines complémentaires, notamment l'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, et l'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.

La législation relative à la protection des droits de propriété intellectuelle notamment les articles L335-1 à 335-10 du Code de la propriété intellectuelle : les dispositions interdisent notamment à tout utilisateur de réaliser des copies de logiciels commercialisés, pour quelque usage que ce soit, ainsi que de dupliquer, distribuer ou diffuser des documents (images, sons, vidéos,...) protégés, ou d'altérer la protection d'une œuvre, d'un phonogramme, d'un vidéogramme ou d'un programme par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle.

La législation relative à la protection des données à caractère personnel, notamment les articles 50 à 52 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers e taux libertés : les infractions aux dispositions de la loi de 1978 sont prévues et réprimées par les articles226-16 à 226-24 du code pénal.
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 2004-801 du 6 août 2004 (cf. articles 226-16 à 226-24 et R625-10 du code pénal).
Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dite "loi Godfrain" (cf. articles323-1 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.

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, a étendu aux logiciels en tant qu'œuvres de l'esprit, la protection prévue par la loi n° 57-298 du 11 mars 1957 sur la propriété littéraire et artistique. (cf. **Code de la Propriété Intellectuelle**, œuvres définies par l'article L112-2, articlesL335-2 et suivants sur la contrefaçon des œuvres de l'esprit, article L521-1 et suivants sur la contrefaçon des dessins ou modèles nationaux, article L713-1 et suivants sur la protection des marques).
Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et le **décret n° 2011-219** relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.
Loi n° 2009-669 du 12 juin 2009 a créé l'HADOPI chargée 1) de protéger les œuvres à l'égard des actes de contrefaçon numérique 2) encourager le développement de l'offre légale et observer l'utilisation licite et illicite des œuvres 3) assurer une régulation et une veille dans le domaine des mesures techniques ; complétée par la loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet.