Charte Informatique de l'ISETA-ECA

(Validée par le directeur de l'établissement le 23 juin 2022)

Ce texte, associé au règlement intérieur de l'institut, est avant tout un code de bonne conduite. Il a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation, afin d'instaurer un usage correct des ressources informatiques et des services Internet, avec des règles minimales de courtoisie et de respect d'autrui.

Sommaire

1. Champ d'application de la charte

Les règles et obligations ci-dessous énoncées s'appliquent à toute personne, en particulier enseignants, étudiants, personnels administratifs ou technique, autorisée à utiliser les moyens et systèmes informatiques de l'ISETA-ECA.

Elle sera signée par toute personne travaillant, étudiant ou accueillie dans chaque site de l'institut, et ayant accès au dit système.
En outre les utilisateurs ne respectant pas les règles et obligations définies dans cette charte seront passibles de sanctions internes à l'établissement dans le respect des procédures disciplinaires statutaires propres aux agents concernés.

Enfin, tout utilisateur n'ayant pas respecté la Loi pourra être poursuivi pénalement dans le cadre des atteintes aux systèmes de traitement automatisé de données, défini en particulier aux articles 121.1 à 121.7 du Code Pénal.(cf Annexe page 12).

La CNIL, Commission Nationale de l'Informatique et des Libertés, est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle exerce ses missions conformément à la loi nº 78-17 du 6 janvier 1978, modifiée le 6 aout 2004.

Par "système d'information" s'entend l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunication, pouvant être mis à disposition par l'institution. Il comprend notamment les serveurs, stations de travail et micro-ordinateurs des services administratifs, des salles de cours ou d'informatique, des laboratoires et des Centres de Documentation.

Le respect des règles définies par la présente charte s'étend également à l'utilisation des systèmes informatiques d'organismes extérieurs à l'institut, systèmes accessibles par l'intermédiaire des réseaux de l'établissement, par exemple le réseau Internet.

L'informatique nomade (assistants personnels, smartphones, ordinateurs portables, téléphones portables,…) est également un des éléments constitutifs du système d'information, dans la mesure où il accède au système via Wifi.

2. Protection des données à caractère personnel

Dans le cadre du nouveau règlement européen sur la protection des données personnelles (RGPD), il est porté à la connaissance de l'utilisateur les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués, ainsi que les règles de confidentialité à respecter.

a. Confidentialité de l'information et obligation de discrétion

Le personnel et les étudiants sont soumis au secret professionnel. L'utilisateur doit assurer la confidentialité des données qu'il détient.
Un comportement exemplaire est exigé dans toute communication orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés. Il est ainsi interdit de prendre connaissance des informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courrier électroniques dont l'utilisateur n'est ni directement destinataire, ni en copie.
L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ou confidentielles.

b. Droit d'accès et rectification

Le RGPD ouvre aux personnes concernées par ces traitements, un droit d'accès et de rectification des données enregistrées sur leur compte. Nous recensons, dans un registre, la liste de l'ensemble des traitements de données à caractère personnel de l'établissement au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande.
L'ISETA-ECA veille particulièrement au respect des droits des personnes (droit d'accès, de rectification et d'opposition).

3. Conditions d'accès aux réseaux informatiques de l'institut

a. Utilisation des ordinateurs de l'institut

L'utilisation des moyens informatiques de l'institut a pour objet exclusif de mener des activités de recherche, d'enseignement ou d'administration. Sauf autorisation préalable délivrée par l'institut, ces moyens ne peuvent être employés en vue d'une utilisation ou de la réalisation de projets ne relevant pas des missions de l'institut ou des missions confiées aux utilisateurs.

L'utilisation d'internet à des fins autres que professionnelles doit être faite avec un usage raisonnable, non susceptible d'amoindrir les conditions d'accès au réseau et ne mettant pas en cause la productivité.
Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace.

Chaque utilisateur se voit attribuer des codes d'accès (un nom d'utilisateur et un mot de passe), en fonction de ses besoins (accès internet, accès aux applications de gestion, accès à des serveurs particuliers, etc.). Les codes d'accès attribués sont strictement personnels et incessibles. Chaque utilisateur est responsable de l'utilisation qui en est faite. Chaque utilisateur s'engage à ne pas communiquer ces codes à une tierce personne.
L'utilisateur préviendra le responsable informatique si un code d'accès ne lui permet plus de se connecter ou s'il soupçonne que son compte a été usurpé. D'une façon plus générale, il informera le responsable informatique de toute anomalie qu'il pourrait constater.

b. *Cas particulier des matériels informatiques personnels des utilisateurs*

i. Raccordement par câble réseau

Toute connexion <u>filaire</u> au réseau local de l'institut à partir d'un matériel informatique personnel est interdite.

---

ii. Raccordement Wifi (réseau sans fil)

L'accès à Internet via des bornes de diffusion Wifi est disponible sur les sites de Poisy et Sevrier dans les lieux suivants :

- Salles de cours de tous les bâtiments.
- CDI
- Chambres d'internat
- Salles de réunion des bâtiments administratifs

Cet accès est autorisé pour :

- Les personnels de l'établissement possédant un ordinateur portable de l'ISETA-ECA.
    - Ils se connectent automatiquement au réseau Wifi « WIFI-PERSONNELS »
        - Durée et plages horaires de connexion : illimité

- Les élèves et les personnels de l'établissement, via leurs propres ordinateurs ou smartphones.
    - Ils se connectent via un portail d'identification au réseau Wifi « WIFI-PEDAGOGIQUE »
    - Les identifiants de connexion sont les mêmes que ceux utilisés sur les ordinateurs de l'ISETA-ECA mis à disposition des élèves.
    - Ces codes sont nominatifs, et sont donnés à chaque étudiant en début d'année.
        - Durée et plages horaires de connexion : 8h-22h. Déconnexion automatique toutes les 2h.
        - Filtrage des sites internet et applications illicites : oui.

- Les visiteurs de l'établissement.
    - Ces personnes doivent se rendre à l'accueil du site afin d'obtenir des codes d'accès spécifiques et faire l'objet d'un enregistrement de leur nom.
        - Durée et plages horaires de connexion : les codes d'accès sont valables jusqu'à minuit.

4. Respect des règles de la déontologie informatique

Chaque utilisateur, qui est juridiquement responsable de l'usage qu'il fait des ressources informatiques, s'engage à respecter les règles de la déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- de masquer sa véritable identité ;
- de s'approprier le mot de passe d'un autre utilisateur ;

- d'altérer, de modifier des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau 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 ;
- d'interrompre ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau ;
- de modifier ou de détruire des informations sur un des systèmes ;

La réalisation d'un programme informatique ayant de tels objectifs est également interdite.

5. Utilisation de logiciels

L'utilisateur ne peut installer un logiciel sur un poste de l'institut, qu'après avis du service informatique compétent. L'utilisateur ne devra en aucun cas :

- installer des logiciels à caractère ludique ;
- faire une copie d'un logiciel commercial ;
- contourner les restrictions d'utilisation d'un logiciel ;
- développer des programmes constituant ou s'apparentant à des virus.

6. Utilisation de données géographiques mises à disposition

L'utilisateur s'engage à n'exploiter ces fichiers et les données qu'ils contiennent, sous toute forme et sous tout support, que dans le cadre de sa formation à l'ISETA-ECA et s'interdit toute autre utilisation.

Il s'interdit toute reproduction aux fins de divulgation, communication, mise à disposition, transmission des fichiers et des données à des tiers, sous toute forme, sur tout support, par quelque moyen et pour quelque motif que ce soit, à titre gratuit ou onéreux.

7. Utilisation des moyens informatiques

Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il doit informer le service informatique de toute anomalie constatée. L'utilisateur doit s'efforcer de n'occuper que la quantité d'espace disque qui lui est strictement nécessaire. L'utilisation des ressources doit être rationnelle et loyale afin d'en éviter la saturation.
Tout ordinateur propre à un département, laboratoire ou service, doit être connecté au réseau par l'intermédiaire d'un informaticien de l'ISETA-ECA. Ce dernier s'assure en particulier que les règles de sécurité sont bien respectées.

8. Dispositions particulières pour les utilisateurs étudiants et professeurs (utilisateurs hors administratif)

a. ENT (Environnement numérique de travail) Ecole Directe

Dans le souci constant d'améliorer les services offerts aux étudiants, l'institut, offre, aux professeurs et élèves, ainsi qu'aux familles qui le souhaitent, la possibilité de gérer et de suivre les résultats scolaires des étudiants, en direct sur Internet, via le site Web « Ecole Directe».

Ces utilisateurs peuvent également consulter l'état des absences, des retards, des sanctions, des stages et obtenir des informations pratiques sur la vie de l'institut.

Cet outil informatique a été créé par APLIM France, qui est la cellule informatique de l'Enseignement Catholique, à qui on doit déjà l'utilisation dans notre institut, du système de gestion de notes des élèves, Charlemagne.

APLIM s'est engagé auprès de la CNIL (*Commission Nationale de l'Informatique et des Libertés*), à respecter les droits et obligations d'accès, de sécurité et de confidentialité des données publiées sur son site Internet.
Le nom de domaine du site Ecole Directe (http:\\www.ecoledirecte.com) a fait l'objet d'une déclaration d'existence à la CNIL.

b. Usage des services Internet (web, messagerie, forum...)

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles ou scolaires et dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.
En particulier :

- il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités ;
- il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- il ne doit pas usurper l'identité d'une autre personne ;
- il ne doit pas intercepter de communications entre tiers et il a l'obligation de s'abstenir de toute ingérence dans la transmission des messages en vertu du secret des correspondances privées ;
- il ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- il ne doit pas déposer des documents sur un serveur sauf si celui-ci le permet ou sans y être autorisé par les responsables habilités ;
- il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions...
- il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'institut ;
- il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère illicite, injurieux, raciste, pornographique, diffamatoire.

i. Filtrage des accès Internet

Afin de garantir le respect et l'application de ces règles, le réseau informatique Wifi de l'institut est équipé d'un système d'authentification et de filtrage de sites, basé sur les technologies d'UCOPIA et l'appliance FORTINET.
Les requêtes (pages demandées par l'utilisateur) sont contrôlées et analysées par un serveur dédié. Toute demande non conforme est rejetée et l'utilisateur averti par l'affichage sur son poste d'une page Web lui indiquant les raisons de ce blocage.

De plus, la requête bloquée est inscrite dans un fichier qui peut permettre de remonter à l'utilisateur en cause si une demande en est faite par la Police ou la Gendarmerie (en cas d'accès à des sites web interdits par la loi par exemple). L'institut est tenu légalement de pouvoir fournir ce genre d'informations en cas d'enquête par les services compétents. (Décret d'application 2006-358 2006-03-24 JORF du 24 mars 2006).

ii. Messagerie Microsoft Office 365 pour l'éducation

L'institut offre aux étudiants, un service de messagerie électronique à usage « professionnel » et « scolaire » permettant d'établir une communication interne ou externe entre les différents élèves, professeurs, et personnels administratifs, basé sur les technologies Microsoft Office 365.
Il s'agit d'une offre de services en ligne, hébergée par Microsoft, et réservée au monde de l'éducation, sans publicité.
Au-delà de la messagerie électronique, Microsoft Office 365 inclut de nombreux autres services créés pour permettre aux enseignants et étudiants de communiquer et de travailler ensemble.

Engagements des utilisateurs

Les utilisateurs s'engagent à n'utiliser le service de messagerie d'Office 365 que :
• dans le respect des lois relatives à la propriété littéraire et artistique ;
• dans le respect des lois relatives à l'Informatique aux fichiers et aux libertés ;
• dans le respect des règles relatives à la protection de la vie privée et notamment du droit à l'image d'autrui,
• en s'assurant de ne pas envoyer de messages à caractère raciste, pornographique, pédophile, injurieux, diffamatoire… et de manière générale à ne pas diffuser d'informations présentant le caractère d'un délit.

Les utilisateurs s'engagent à n'utiliser le service de stockage en ligne Onedrive ou Sharepoint qu'en y publiant des documents autorisés par la loi et le copyright.

9. Information des utilisateurs sur la gestion des systèmes et réseaux informatiques

a. Responsabilités des administrateurs systèmes/réseau

Les administrateurs systèmes/réseau sont des ingénieurs ou techniciens informatiques, qui gèrent les machines connectées aux réseaux des sites de l'ISETA-ECA, ainsi que les serveurs sur lesquels sont installés les différents services mis à la disposition des utilisateurs (services internet, applications de gestion, services pédagogiques, services pour la recherche et la documentation).

L'équipe informatique est actuellement constituée de 2 personnes :
- Samuel Noailhet, Responsable informatique
- Christophe Domenjoud, technicien informatique.

- Les administrateurs ont la charge de la bonne qualité du service fourni aux utilisateurs dans la limite des moyens alloués. Ils ont le droit d'entreprendre toute démarche nécessaire au bon fonctionnement des moyens informatiques de l'institut ;
- Les administrateurs ont le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques ;
- Les administrateurs ont le devoir d'informer immédiatement le responsable de cycle (ou son suppléant) de toute tentative d'intrusion sur un système, ou de tout comportement délictueux d'un utilisateur ;
- Les administrateurs doivent impérativement respecter la confidentialité des fichiers des utilisateurs.

b. Fichiers de traces

L'ensemble des services utilisés génère, à l'occasion de leur emploi, "des fichiers de traces". Ces fichiers sont essentiels à l'administration des systèmes. Ils servent en effet à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations par exemple concernant la messagerie (expéditeur, destinataire(s), date), mais aussi heures de connexion aux applications de gestion, au service de connexion à distance, numéro de la machine depuis laquelle les services sont utilisés, etc.
Ce type de traces existe pour l'ensemble des services internet. Ces fichiers ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'une procédure judiciaire et après accord de la direction, ces fichiers peuvent être mis à la disposition ou transmis à la justice.

c. Les virus

Des outils sont également mis en place pour protéger les postes des utilisateurs contre les virus.

- Les logiciels anti virus sur les postes des utilisateurs sont paramétrés avec la stratégie suivante : Si un virus est détecté, le logiciel tente de réparer le fichier, si la tentative échoue, le fichier est détruit.
- Un logiciel d'anti virus est également mis en place sur les serveurs de messagerie évitant ainsi de recevoir des virus et aussi d'en émettre à l'extérieur. Le destinataire et l'expéditeur sont informés que le message contenait un virus et le message n'est pas délivré.
- D'autres logiciels pourront être mis en place pour protéger au mieux les données des utilisateurs et les applications de l'institut.
- En ce qui concerne l'accès au réseau Wifi, et notamment par les matériels personnels des utilisateurs, notre cœur de réseau reste protégé grâce à l'appliance FORTINET.

Cas spécifiques des matériels personnels des utilisateurs

L'ISETA-ECA se dégage de toute responsabilité quant à l'éventuelle infection virale d'un matériel personnel, et ce, même si celui-ci accède à Internet par le réseau Wifi de l'ISETA-ECA.
C'est à l'utilisateur, et à lui seul, qu'il incombe de se protéger en mettant en place un logiciel de protection antivirus et antispyware.

De plus, toute connexion via le réseau Wifi de l'ISETA-ECA étant enregistrée, un poste utilisateur infecté ou téléchargeant des documents illicites, pourra être bloqué définitivement, et ainsi ne plus avoir accès au réseau Wifi de l'ISETA-ECA. Son détenteur s'engage également à des sanctions internes, et pénales le cas échéant.

10. Procédure applicable lors du départ de l'utilisateur

Lors de son départ, l'utilisateur doit restituer au service de l'informatique interne les matériels mis à sa disposition.
Il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par le chef de service.
Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ.

11. Sanctions

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose au retrait de son compte informatique, ainsi qu'aux poursuites disciplinaires et pénales, prévues par les textes législatifs et réglementaires en vigueur.

Formulaire d'adhésion à la charte informatique de l'ISETA-ECA

Je soussigné,

Nom : _

Prénom : _

Qualité : ☐ Employé ☐ Vacataire ☐ Etudiant
☐ Lycéen ☐ Apprenti ☐ Stagiaire

Utilisateur des moyens informatiques et réseaux des sites de l'ISETA-ECA, déclare avoir pris connaissance de la présente charte de bon usage de l'informatique et des réseaux et m'engage à la respecter.

Fait à Le	Signature, précédée de la mention « lu et approuvé »

Annexes : code pénal

CODE PENAL
(Partie Législative)
Des atteintes aux systèmes de traitement automatisé de données

Article 323-1

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)
(Loi n° 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)
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.

Article 323-2

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)
(Loi n° 2004-575 du 21 juin 2004 art. 45 II Journal Officiel du 22 juin 2004)
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.

Article 323-3

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)
(Loi n° 2004-575 du 21 juin 2004 art. 45 III Journal Officiel du 22 juin 2004)
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.

Article 323-3-1

(inséré par Loi n° 2004-575 du 21 juin 2004 art. 46 I Journal Officiel du 22 juin 2004)
Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4

(Loi n° 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 juin 2004)
La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5

Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1º L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2º 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 ;

3º La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4º La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5º L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6º L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7º L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :

1º L'amende, suivant les modalités prévues par l'article 131-38 ;

2º Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2º de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7

(Loi nº 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 juin 2004)

La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.