

CHARTRE INFORMATIQUE

Chapitre I - Généralités

Art. 1 Introduction

¹ Cette charte fixe les règles fondamentales assurant une utilisation optimale des moyens informatiques mis à disposition des élèves, des enseignants et des intervenants externes de l'établissement.

² Ces règles complètent celles de la législation en vigueur, relatives notamment à la fraude informatique, à la protection du droit d'auteur et à la protection des données. Qu'elles soient cantonales ou fédérales.

³ Dans ce document, l'emploi du masculin pour désigner des personnes n'a d'autres fins que celles d'alléger le texte.

Art. 2 Périmètre

¹ Le périmètre de cette charte englobe l'ensemble des ressources informatiques pédagogiques de l'établissement. Demeure réservée la charte établie par la DSI concernant les ressources informatiques administratives.

² Par ressources, on entend : tous les postes informatiques connectés ou non au réseau, le réseau informatique ethernet et le réseau wifi, ainsi que tous les logiciels installés sur les postes

³ L'utilisation de matériel privé (ordinateur, smartphone, tablettes, etc) est également soumise à la présente charte, pour autant qu'il soit autorisé au sein de l'établissement, et quel que soit le réseau utilisé (sans fil ou filaire).

Art. 3 Champ d'application

¹ Le présent règlement s'applique au personnel, aux élèves et aux intervenants externes, utilisant le réseau pédagogique.

² Est entendu par "le personnel" : les membres du corps enseignant, les membres du personnel administratif et technique de l'établissement, pour autant qu'ils utilisent les ressources informatiques pédagogiques.

³ Est entendu par "les élèves" : les élèves suivant leurs études dans l'une des filières de l'établissement. Quelque soit le type de formation suivie.

⁴ Est entendu par "les intervenants externes" : tous les usagers occasionnels, autorisés par la direction de l'établissement, utilisant les ressources informatiques de l'établissement ou leur matériel personnel.

Art. 4 Engagement des usagers

¹ Par sa signature, l'utilisateur, quelle que soit la catégorie (art. 3), s'engage à suivre et respecter le règlement décrit dans cette charte.

² Par son comportement, l'utilisateur engage sa responsabilité vis-à-vis des actes perpétrés sous son compte d'accès, s'ils vont à l'encontre de la présente charte.

³ Les utilisateurs s'engagent à ne pas diffuser des informations qui peuvent ternir la réputation de l'établissement ou être contraires à la morale et aux lois en vigueur.

Art. 4.1 Signature

¹ Si l'utilisateur est mineur au moment de la signature, la charte sera signée par le représentant légal de l'utilisateur, en plus de sa propre signature.

Art. 4.2 Validité

¹ La validité de cet engagement prend fin lorsque l'utilisateur quitte l'établissement définitivement, d'un point de vue administratif.

Art. 5 Droit d'accès aux ressources

¹ Le droit d'accès aux ressources et système d'information de l'établissement n'est accordé qu'après avoir pris connaissance et signé la présente charte.

² L'utilisateur a le devoir de transmettre des informations personnelles exactes et complètes lors de la création de son compte. Il a l'obligation de tenir à jour ces informations régulièrement, tout au long de son engagement envers l'établissement.

Art. 6 Sanctions

¹ En cas d'abus ou de non-respect de cette charte, des mesures pourront être prises à l'encontre du contrevenant avéré. Les sanctions peuvent varier du simple blâme à l'exclusion de l'établissement, voire aboutir au dépôt d'une plainte pénale.

² La prise de décision appartient à l'établissement, selon la faute commise, sous la responsabilité du Directeur.

³ Toute déprédation de matériel informatique, intentionnelle ou par négligence, sera sanctionnée.

⁴ Le vol de ressources informatiques (matériel ou logiciel) est, comme tout vol, un acte répréhensible et de ce fait des poursuites pénales pourraient en être une des conséquences.

Chapitre II – Personnes, données et vie privée

Art. 7 Respect des personnes et de la sphère privée

¹ L'utilisateur s'engage à respecter les règles juridiques en vigueur, notamment les articles 135, 173, 174, 177, 197, 261 et 261b du Code Pénal. Il est formellement interdit de consulter, créer, stocker ou diffuser des documents qui pourraient :

- a) porter atteinte à la dignité des personnes.
- b) illustrer avec insistance des actes de cruauté, constituer une apologie du crime et de la violence, au sens de l'article 135 CP.
- c) présenter un caractère pornographique, au sens de l'article 197 CP sus cité, et par analogie, un caractère pédophile ou zoophile
- d) porter atteinte à la liberté de croyance et des cultes, au sens de l'article 261 CP.
- e) inciter à la haine ou à la discrimination raciale, au sens de l'article 261bis CP,
- f) propager des propos diffamatoires, calomnieux ou injurieux (art. 173, 174 et 177 CP)

² Cet article s'applique à tout document circulant dans l'établissement, qu'il soit rédigé ou juste consulté par l'utilisateur, exception est admise dans le cas de consultation répondant à un besoin d'enseignement.

³ Si par mégarde, un tel document s'affiche à l'écran, l'élève est tenu d'en informer immédiatement l'enseignant présent ou le répondant informatique de l'établissement, directement ou par moyen électronique (mail, par exemple).

⁴ Il est interdit de diffuser des informations personnelles relatives à d'autres utilisateurs sans leur consentement, quels que soient les outils et l'appartenance des ressources utilisées. L'utilisation des ressources informatiques à disposition ne peut en aucun cas servir à nuire à une autre personne.

⁵ Il est interdit de chercher à consulter le courrier électronique d'un autre utilisateur, d'accéder à ses fichiers ou de lui emprunter son compte d'accès.

Art. 8 Droit à l'image et droit de la personnalité

¹ Les utilisateurs s'engagent à respecter, de manière absolue, le droit de la personnalité de chacun, notamment le droit à l'image, comme décrit dans l'article 28 du code civil Suisse.

Art. 9 Protection des données

¹ De par certaines de ses fonctions et activités, le personnel et les intervenants externes pourraient avoir accès à des données personnelles et/ou confidentielles. S'appliquent alors les règles soumises par la Lpers.

Art. 10 Protection des droits d'auteur

¹ Les utilisateurs s'engagent à ne pas diffuser des informations appartenant à des tiers sans leur autorisation et dans tous les cas, à mentionner les sources lors de l'utilisation d'informations de tiers. (loi sur les droits d'auteurs du 01.07.1993)

² La copie de support média protégés par un copyright est interdite. Par extension, si un support semble ne pas être original (piratage), il est de la responsabilité de l'utilisateur de le considérer comme une œuvre protégée par un copyright.

³ Le téléchargement d'œuvres protégées, par l'utilisation de médias, de sites ou logiciels de téléchargement et de partage de médias (de type peer-to-peer et direct download), est interdit. Si les utilisateurs outrepassent cette interdiction, ils engagent directement la responsabilité de l'établissement. Cette interdiction est valable également lors de l'utilisation d'ordinateur ou de matériel ultraportable privé appartenant à l'utilisateur, que l'ordinateur soit connecté au réseau ethernet ou au réseau wifi de l'établissement.

⁴ Conformément à la nouvelle loi sur les droits d'auteur (LDA), article 2 alinéa 3, il est interdit de copier des logiciels appartenant à l'école pour les enregistrer sur son ordinateur personnel ou sur un support quelconque et d'en disposer hors de l'école sans autorisation, qu'il s'agisse des originaux ou de copies. La copie et le piratage de logiciel sont interdits.

Chapitre III – Utilisation des moyens informatiques

Art. 11 Utilisation des moyens informatiques

¹ Les règles d'usage de l'établissement s'appliquent.

² L'utilisation des ressources informatiques doit se faire dans une perspective pédagogique avant tout. Une utilisation des outils informatiques à titre privé est admise pour autant qu'elle entre dans un cadre légal, qu'elle n'empêche pas un autre utilisateur d'utiliser les ressources pour son travail scolaire et qu'elle ne surcharge pas l'infrastructure (transferts de données, par exemple).

Art. 11.1 Utilisation des salles de la file informatique et des salles en libre accès

¹ Les règles d'usage de l'établissement s'appliquent.

² Il est demandé à chacun d'utiliser avec précaution et respect les ressources qui lui sont mises à disposition par l'école.

Art. 11.2 Utilisation d'internet et de ses moyens

¹ Les règles d'usage de l'établissement s'appliquent.

² Est entendu par "ses moyens" : le mail, les réseaux sociaux, les applications, les jeux en ligne, etc.

³ Les activités liées à l'utilisation d'internet sont tracées et contrôlées régulièrement.

⁴ L'utilisation du courrier électronique est réservée aux besoins pédagogiques. Une utilisation privée peut être autorisée, à condition qu'elle n'enfreigne pas la règle décrite à l'article 7 alinéa 1, qu'elle ne surcharge pas l'infrastructure informatique et ne vise aucun but lucratif.

⁵ Chaque message transmis doit mentionner le nom de son auteur.

⁶ Par définition, le chat est interdit car l'utilisation de pseudo va à l'encontre de l'alinéa 5 du présent article.

⁷ L'utilisateur s'engage à ne pas modifier les paramètres techniques de la messagerie.

Art. 11.3 Modification et déplacement du matériel

¹ Sauf cas exceptionnel d'enseignement et de formation autorisé, il est interdit de :

a) modifier la configuration du poste en retirant ou installant des composants ou périphériques (graveur, disque supplémentaire, lecteur dvd, modem, etc.)

b) modifier la configuration logicielle du poste en ajoutant ou retirant des programmes, en désactivant des protections etc.

c) connecter au poste de travail ou sur le réseau des appareils électroniques non explicitement autorisés (smart phone, iPad et autres tablettes, console de jeu, etc.)

d) installer des programmes téléchargés par internet, reçus par mail ou en provenance de toute autre source

e) réaliser des développements informatiques.

² Les modifications effectuées, interdites au sens de l'alinéa 1 du présent article, seront supprimées sans préavis.

³ L'utilisateur ne prendra aucune initiative d'ordre technique sur les postes de travail. De la même manière, il est interdit de modifier le câblage, sauf sur demande du responsable du réseau.

⁴ Le matériel informatique ne doit pas être déplacé, sauf sur demande de l'enseignant responsable.

Art. 11.4 Serveurs de fichiers

¹ Les règles d'usage de l'établissement s'appliquent.

Art. 11.5 Utilisation de matériel privé

¹ L'utilisation de matériel informatique personnel (par exemple : ordinateur portable, smartphone, tablette, etc.) est soumise à autorisation accordée par les responsables de l'établissement, quel que soit le réseau avec lequel il se connecte (wifi ou filaire), selon les règles d'usage de l'établissement.

Art. 11.6 Pannes et dysfonctionnements

¹ L'utilisateur informe immédiatement le responsable de l'informatique de l'établissement en cas de constatation d'anomalie ou en cas d'incident.

Chapitre IV – Sécurité informatique

Art. 12 Droits d'accès, compte utilisateur et mot de passe

¹ Les utilisateurs reçoivent un nom d'utilisateur et un mot de passe qui constitue leur compte informatique permettant d'accéder aux ressources informatiques. La responsabilité de l'usager est engagée dès l'introduction de son mot de passe jusqu'à la fin de la session de travail.

² Ce droit d'accès est personnel et intransmissible et le mot de passe doit être gardé secret par son propriétaire. Tout comme il est interdit de se servir de la session ou du compte d'un autre utilisateur.

³ Le mot de passe choisi par l'utilisateur ne doit correspondre ni à un mot, ni à un nom propre d'aucune langue que ce soit, ni être une dérivation simple d'un tel mot. Le mot de passe doit comporter au moins 8 caractères, composé d'au moins un chiffre et un caractère spécial.

⁴ Lorsqu'un usager a fini sa session, il a l'obligation de se déconnecter. Il est interdit de bloquer un poste (lock station) et de s'en aller, dans le but de réserver une place de travail.

⁵ Il est interdit de se connecter simultanément, avec le même compte, sur plusieurs postes

Art. 13 Système et logiciels

¹ L'utilisateur s'engage à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquence d'interrompre, sans y être autorisé, le fonctionnement normal du réseau ou d'un des composants connectés au réseau. La réalisation d'un programme informatique ayant de tels objectifs est également interdite. Tout acte qui pourrait mettre en cause le fonctionnement des installations informatiques est strictement prohibé. Il est également interdit de procéder à un audit des infrastructures ou de récupérer le trafic transitant sur le réseau.

² Il est interdit de modifier les configurations des systèmes d'exploitation

³ Seuls les logiciels déjà présents sur les ordinateurs peuvent être utilisés.

⁴ Il est interdit de démarrer l'ordinateur avec une clef USB branchée ou un CD / DVD dans le lecteur de disque. L'ordinateur ne doit pas être démarré avec un autre système d'exploitation que celui installé par les soins d'un répondeur informatique. Toute tentative sera assimilée à un piratage du réseau informatique.

Art. 14 Contournement des mesures de sécurité mises en place

¹ Toute activité et toute manœuvre destinée à contourner les systèmes de sécurité (logiciels et matériels) sont interdits. L'exploitation de failles permettant le contournement du système de protection est également strictement interdite.

Art. 15 Virus et anti-virus

¹ Les utilisateurs prendront toutes les mesures nécessaires pour éviter l'intrusion de virus. En cas de pièces jointes dans un mail, l'utilisateur est responsable des dégâts provoqués par son ouverture. Il prendra également soin de vérifier la source de l'envoi.

² Les utilisateurs s'engagent à ne pas désactiver la protection antivirus, ni à essayer de contourner ou désactiver les logiciels de supervision installés sur les postes.

Art. 16 Connexion avec des réseaux externes à l'établissement

¹ Pour des raisons de protection contre des risques externes, il n'est pas autorisé d'utiliser un ordinateur pour créer un pont vers un autre système ou réseau.

² L'utilisateur s'engage à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquence de se connecter ou d'essayer de se connecter à d'autres systèmes ou réseaux (externes) sans y être autorisé.

³ L'utilisateur ne cherchera pas à porter atteinte à d'autres sites. La réalisation d'un programme informatique ayant de tels objectifs est également interdite

Art. 17 Sauvegarde des données (selon les règles de chaque établissement)

¹ L'établissement ne garantit ni la sauvegarde, ni l'intégrité des données stockées sur les disques internes des machines individuelles ou des périphériques rattachés, ni même sur les serveurs. Il est indispensable de procéder régulièrement à une sauvegarde sur DVD, disque dur externe ou clé USB.

² Les règles d'usage de l'établissement s'appliquent.

Chapitre V – Contrôles

Art. 18 Contrôles

¹ Des contrôles du respect de la présente charte seront effectués à différents niveaux.

² Les administrateurs du système disposent des autorisations permettant de contrôler l'utilisation du système. Ils sont tenus au devoir de discrétion, mais peuvent explorer les fichiers des utilisateurs et en faire connaître le contenu à la direction de l'établissement si des abus sont constatés. Les activités sur internet peuvent également faire l'objet de contrôles.

Par ma signature, je certifie que je sais :

- comment accéder à mon compte eduvaud
- comment dévier mon courrier sur une autre adresse mail

Je m'engage également à :

- consulter régulièrement ma boîte électronique
- et à la vider de temps à autre,

de manière à pouvoir recevoir en tout temps les mails envoyés par le secrétariat ou la Direction.