**Gymnase de Beaulieu**
Rue du Maupas 50
Case postale 356
1000 Lausanne 22

# CHARTE INFORMATIQUE

version mars 2017

## 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 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 de l'établissement.**

[2] **Par ressources, on entend : tous les postes informatiques connectés ou non au réseau, le réseau informatique filaire et le réseau sans fil, les logiciels installés sur les postes ainsi que l'adresse de courrier électronique fournie par le gymnase.**

[3] **L'utilisation de matériel privé (ordinateur, smartphone, tablette, etc.) est également soumise à la présente charte quel que soit le réseau utilisé (sans fil ou filaire).**

### Art. 3 Champ d'application

[1] **Le présent règlement s'applique aux élèves utilisant le réseau informatique.**

[2] **Est entendu par "les élèves" : les élèves suivant leurs études dans l'une des filières de l'établissement, quel que soit le type de formation suivie.**

### Art. 4 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, logiciel ou données) 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. 5 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 notamment interdit de consulter, créer, stocker ou diffuser des documents comportant les éléments suivants :**

- **a) l'atteinte à la dignité des personnes ou les délits contre l'honneur (diffamation, calomnies, injures, allégations nuisant au commerce ou à la solvabilité, notamment les infractions à la LCD ;**
- **b) l'illustration avec insistance des actes de cruauté, l'apologie du crime et de la violence ou leur incitation ;**
- **c) la pornographie, notamment à caractère pédophile ou zoophile ;**
- **d) l'atteinte à la liberté de croyance et des cultes ;**
- **e) l'incitation à la haine ou à la discrimination raciale ;**
- **f) l'incitation à toute autre discrimination à l'égard d'autres personnes ;**
- **g) l'incitation à commettre des actes répréhensibles ;**
- **h) les jeux de hasard payants.**

[2] **L'utilisateur s'engage à ne pas consulter, créer, stocker ou diffuser des documents contraires à l'éthique de l'établissement ou qui pourraient nuire à son image.**

[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 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. 6 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.**

## Chapitre III – Utilisation des moyens informatiques

### Art. 7 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 (transfert de données, par exemple).

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

### Art. 8 Configuration informatique

[1] Il est interdit de :

a) modifier la configuration logicielle et matérielle des postes ;

b) connecter au poste de travail ou sur le réseau des appareils électroniques non explicitement autorisés ;

c) 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. 9 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. 10 Droits d'accès, compte utilisateur et mot de passe

[1] Les utilisateurs reçoivent un nom d'utilisateur et un mot de passe qui constituent 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.

[3] Il est interdit de se servir de la session ou du compte d'un autre utilisateur.

[4] Il est interdit de se connecter simultanément, avec le même compte, sur plusieurs postes.

[5] 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.

[6] 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.

### Art. 11 Système et logiciels

[1] L'utilisateur s'engage à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquence d'interrompre le fonctionnement normal du réseau ou d'un des composants connecté 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 répondant informatique. Toute tentative sera assimilée à un piratage du réseau informatique.

### Art. 12 Contournement des mesures de sécurité mises en place

[1] Toute activité et toute manœuvre destinées à contourner les systèmes de sécurité (logiciels et matériels) sont interdites. L'exploitation de failles permettant le contournement du système de protection est également interdite, notamment selon les articles 143 et 143 bis CP.

### Art. 13 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'usager ne cherchera pas à porter atteinte à d'autres sites. La réalisation d'un programme informatique ayant de tels objectifs est également interdite

### Art. 14 Sauvegarde des données

[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.

## Chapitre V – Contrôles

### Art. 15 Contrôles

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

[2] Les activités liées à l'utilisation d'internet sont tracées et contrôlées régulièrement.

[3] 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.