

Sommaire

1. Objectif	1
2. Domaine d'application	1
3. Utilisation	1
3.1. Internet	1
3.2. Messagerie électronique	2
3.3. Poste de travail	3
4. Départ d'un-e étudiant-e	4
5. Contrôle et mesures de sécurité	4
5.1. Contrôle et mesures	4
5.2. Traitement des informations	4
5.3. Instances compétentes et sanctions en cas d'abus	4

L'utilisation du genre masculin a été adoptée afin de faciliter la lecture et n'a aucune intention discriminatoire.

1. Objectif

L'objectif de la présente charte est de définir les droits et les devoirs des utilisateurs à propos des moyens de communication (Internet, messagerie électronique) et des postes de travail informatiques mis à leur disposition, de prévenir une utilisation abusive de ces derniers et de régler les conséquences d'éventuels abus.

2. Domaine d'application

Cette charte s'applique à tous les étudiants autorisés à se servir des équipements informatiques.

3. Utilisation

3.1. Internet

- 3.1.1 L'internet doit être consulté par l'utilisateur uniquement dans le cadre des fonctions qui lui sont attribuées.
- 3.1.2. L'utilisation de l'internet à des fins personnelles est autorisée à condition que les ressources consommées soient infimes et que la capacité du réseau ne s'en trouve affectée. La consultation à des fins personnelles doit par définition demeurer occasionnelle et accessoires.
- 3.1.3 La HES-SO se réserve le droit de bloquer, sans préavis, l'accès à certaines catégories de sites internet, notamment :
 - sites de messagerie non professionnelle ;
 - sites de messagerie instantanée (« chat ») ;
 - sites de transactions financières (notamment les sites boursiers) ou ceux payants ;
 - sites de jeux et de paris ;

- sites à caractère érotique, violent, raciste ou contraire aux mœurs de quelque manière que ce soit ;
- sites qui sollicitent trop fortement les systèmes d'information (par ex. connexion à des sites radiophoniques).

3.1.4 Les utilisateurs s'engagent à ne pas copier illégalement des logiciels ou des fichiers protégés par un « copyright » (musique, film, etc.) et à ne pas diffuser des informations appartenant à des tiers sans leur autorisation. Ils s'engagent également à mentionner leurs sources lors de l'utilisation d'informations.

3.1.5 Les utilisateurs n'ont pas l'autorisation de s'abonner à des services d'informations payants, sauf autorisation préalable.

3.2. Messagerie électronique

3.2.1. L'utilisation du courrier électronique comme instrument de communication est réservée aux besoins professionnels. Une utilisation privée est admise à titre exceptionnel, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers) et qu'elle ne viole pas le devoir de fidélité et de diligence de la personne concernée.

3.2.2. La mention suivante doit être utilisée dans les éléments d'adressage, concernant la confidentialité ou le caractère privé/personnel d'un courrier électronique :

CONFIDENTIEL : un courrier électronique dont l'élément d'adressage contient ce mot ne peut être ouvert que par la personne à qui le courrier électronique est destiné (dont le nom figure dans le texte ou fait partie de la désignation de la boîte aux lettres).

Sans aucune précision, le courrier pourra être lu par des tierces personnes.

L'utilisateur est responsable d'informer les personnes susceptibles de lui faire parvenir des messages à caractère privé de la manière de rédiger le titre du message.

3.2.3. L'utilisation de fonctionnalités spéciales pour la messagerie (envoi automatique de notification de réception de messages, envoi de SMS, etc.) est réservée exclusivement à des buts professionnels, dans la mesure où elle ne surcharge pas l'infrastructure électronique. L'utilisateur s'engage notamment à ne pas contribuer à la propagation de chaînes de distribution.

3.2.4. L'utilisateur s'assure de la source des fichiers attachés avant de les ouvrir. Les fichiers provenant d'une source inconnue doivent faire l'objet d'une attention particulière (notamment par exemple les extensions : .exe, .com, .bat, .xml, .vbs, .vb). En cas de doute, prendre contact immédiatement avec le service informatique.

3.2.5. Chaque personne s'engage à ne pas modifier les paramètres techniques, ni la liste de contrôles d'accès de sa messagerie personnelle.

3.2.6. L'utilisateur s'engage à ne pas diffuser des informations qui peuvent porter atteinte à la réputation de la HES-SO.

3.2.7. Chaque personne est rendue attentive au fait qu'un courrier électronique peut se transmettre très rapidement et qu'il faut donc être très prudent avec les informations véhiculées, ceci spécialement pour des fichiers attachés à caractère confidentiel.

3.2.8. Si une personne reçoit un courrier électronique à caractère violent, raciste ou pornographique, elle est priée d'en avertir sans délai le service informatique, qui prendra les mesures nécessaires afin de stopper ces réceptions non sollicitées.

3.3. Poste de travail

- 3.3.1. Les seuls postes de travail à disposition sont les postes « professeurs » situés dans les salles de classe. Le poste de travail est un élément constitutif du système informatique de la HES-SO. La modification de son contenu et/ou un usage inapproprié peuvent avoir des effets sur le fonctionnement global du système.
- 3.3.2. Aucun espace de stockage n'est créé afin de permettre aux utilisateurs de stocker des fichiers personnels. Toutefois, les professeurs et les étudiants ont un accès à la plateforme Moodle afin d'échanger les documents de cours.
- 3.3.3. Une utilisation privée des applications installées sur le poste de travail est admise exceptionnellement, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers) et ne viole pas le devoir de fidélité et de diligence de l'utilisateur.
- 3.3.4. Sauf raison justifiée et sans l'accord du SI, il est notamment interdit de :
- modifier la configuration matérielle du poste de travail en retirant des composants ou en installant de nouveaux (par exemple graveur, disque supplémentaire, lecteur DVD, CD-ROM, modem, etc.) ;
 - modifier la configuration logicielle du poste de travail en retirant des programmes ;
 - réaliser des développements informatiques.
- 3.3.5. L'installation, respectivement la mise à jour des postes de travail ne couvre que les configurations et logiciels standards définis par le SI. Les logiciels installés par les utilisateurs et qui ne font pas partie de la configuration standard doivent être maintenus par eux, sans le support du SI. En cas de problème généré par l'un de ces logiciels, le SI réinstallera la plateforme standard sans délai.
- 3.3.6. L'utilisateur ne consulte, ni ne stocke ou ne diffuse des informations qui, sous quelque forme que ce soit, constituent notamment une participation à un acte illicite ou qui, en particulier, portent atteinte à la dignité de la personne, présentent un caractère pornographique, incitent à la haine raciale ou constituent une apologie du crime ou de la violence.
- 3.3.7. L'utilisateur s'engage à traiter son mot de passe personnellement et de manière confidentielle.
- 3.3.8. L'utilisateur s'engage à ne pas désactiver les protections.
- 3.3.9. De manière générale, l'utilisateur stocke ses données sur les serveurs prévus à cet effet. Chaque personne est tenue de les épurer régulièrement.
- 3.3.10. L'utilisateur verrouille son poste de travail en quittant sa place. A la fin de la journée, chaque personne éteint son poste de travail et son écran.
- 3.3.11. L'utilisateur doit avoir un antivirus installé sur son ordinateur. Il peut en télécharger un (gratuitement) sur Internet.

4. Départ d'un étudiant

- 4.1 Lorsqu'une personne quitte la HES-SO, et sans dispositions expresses contraires, son adresse de courrier électronique est immédiatement désactivée.
- 4.2 La personne concernée s'engage à effacer, avant son départ, ses données personnelles de son compte de courrier électronique et de son espace privé.

5. Contrôle et mesures de sécurité

5.1. Contrôle et mesures

- 5.1.1. La HES-SO est attachée au respect de la vie privée de ses étudiants et de son personnel dans ses locaux, et ce en respectant la législation sur la protection des données.
- 5.1.2. L'ensemble du trafic Internet est journalisé. Les utilisateurs sont informés que le personnel du SI (sous la supervision du responsable informatique) peut avoir accès à n'importe quel moment à l'ensemble des composants du système, afin d'assurer sa protection et celle des utilisateurs et/ou déceler des activités illégales.
- 5.1.3. Le personnel du SI procédera à des contrôles anonymes et aléatoires des fichiers journalisés. Le traitement des données relevées est confidentiel et soumis à la protection des données.
- 5.1.4. Le personnel du SI est tenu au secret de fonction et ne peut divulguer, excepté au responsable informatique, ou utiliser à son avantage les informations dont il aurait eu connaissance au cours d'actions de contrôle.

5.2. Traitement des informations

- 5.2.1. En cas d'abus constaté, soit lorsque la présente charte est violée, le responsable informatique procédera à des analyses nominatives des fichiers.

5.3. Instances compétentes et sanctions en cas d'abus

- 5.3.1. Après avoir entendu l'utilisateur et s'il s'avère que l'utilisation d'internet et des moyens informatiques constitue une violation de la présente charte, la HES-SO prend les mesures appropriées telles que par exemple le blocage de la boîte aux lettres ou de l'internet. Ces mesures peuvent aller jusqu'à l'expulsion éventuelle pour justes motifs. Si les agissements de l'utilisateur sont de nature pénale, la HES-SO se réserve tout droit.