



Charte informatique

Préambule	2
Charte	
Le champ d'application	
Les acteurs de la Charte informatique	
La définition des conditions d'accès et d'identification	
Les conditions d'utilisation	
Installation et utilisation de logiciels	5
Internet	5
Messagerie électronique	6
Mobilité et gestion des absences/départs	6
Usage privé des moyens informatiques	7
Réseaux sociaux	7
Sécurité	7
À propos de la traçabilité	7
Contrôle et audit	8
Règles de conservation et de sauvegarde des données	8
Prêt ponctuel de matériel	8
Matériel fourni par l'école aux agents	8
Sanctions et obligations particulières	
Sanctions internes	9
Sanctions civiles	9
Sanctions pénales	9
Propriété intellectuelle	9
Protection des données à caractère personnel	9
Entrée en vigueur	10



La présente Charte définit les règles de bonne utilisation des outils informatiques de la HEAR. Elle a été adoptée par le Conseil d'Administration lors de sa séance du 13 juin 2024.

L'engagement de respect de la présente Charte revêt un caractère impératif pour toute personne utilisant les ressources informatiques de l'école.

Cette première partie a pour objectif de comprendre pourquoi il est nécessaire de mettre en place une Charte informatique.

Préambule

Qu'est-ce qu'une Charte informatique ?

La Charte définit les conditions générales d'utilisation des ordinateurs, accès Internet, des réseaux et des services numériques locaux ou distants.

Ce document recense les droits et obligations des utilisateurs, mais également leurs responsabilités. Elle a pour vocation de vous informer des bonnes pratiques à adopter quant à l'utilisation des outils informatiques de la HEAR. Sa mise en place permet d'éviter toute forme d'abus de l'usage des ressources informatiques et constitue une référence en cas de conflit.

Il faut donc que la Charte soit claire et à la portée de tous.

Pourquoi mettre en place une Charte informatique ?

Elle a pour vocation d'édicter des règles et des comportements conformes à la loi et à la politique de l'établissement. Le non-respect de la charte peut entraîner la responsabilité des utilisateurs.

La Charte informatique est-elle obligatoire ?

La CNIL (Commission nationale informatique et libertés) recommande l'adoption d'une Charte Informatique ayant pour objectif de «sensibiliser les étudiants et personnels aux exigences de sécurité, d'appeler leur attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de l'entreprise ou de l'administration».

La Charte informatique est obligatoire, notamment lors de la collecte des données à caractère personnel et lors de l'installation ou l'exploitation d'outils informatiques propriétaires ou libres.



Charte

La Charte informatique de la HEAR définit les règles de bonne utilisation des ressources numériques. La mise en place de cette Charte a pour vocation de protéger à la fois l'école, l'utilisateur et les administrateurs.

Le champ d'application

Le respect des règles définies par la présente Charte s'étend :

- à l'utilisation des systèmes informatiques de l'école ou d'organismes extérieurs à l'école, accessibles par l'intermédiaire des réseaux publics (Internet...) ou privés (VPN...);
- à l'utilisation de terminaux personnels (Smartphones, ordinateurs portables...) dès lors qu'ils accèdent aux ressources numériques de

la HEAR (Internet, Taïga...).

Les systèmes informatiques de la HEAR comprennent notamment les services en ligne (ex : Taïga), serveurs, stations de travail, ordinateurs portables, terminaux informatiques, systèmes d'impression et de scanners situés dans les services administratifs, les services techniques, les salles informatiques et les bibliothèques.

Les acteurs de la Charte informatique

Les règles et obligations ci-dessous énoncées s'appliquent à toutes les personnes autorisées à utiliser les moyens et systèmes d'informations (« SI ») de la HEAR.

Sont utilisateurs du SI :

- des usagers :
 - > personnels (agents administratifs/ techniques et enseignants),
 - > étudiants ou toute personne en formation à la HEAR (ex : ateliers publics),
 - > personnes externes à la HEAR
- des administrateurs :
 - > les agents du service informatique habilités « systèmes/réseau »,
 - > les enseignants habilités.

Responsabilités des administrateurs:

Les administrateurs :

- ont la charge de la bonne qualité du service fourni aux utilisateurs dans la limite des moyens alloués. Ils entreprennent toute démarche nécessaire au bon fonctionnement des moyens numériques de l'école ;
- 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 numériques ;



- ont le devoir d'informer immédiatement la direction de toute tentative d'intrusion sur un système, ou de tout comportement délictueux d'un utilisateur ;
- doivent impérativement respecter la confidentialité des fichiers des utilisateurs et plus généralement leur vie privée et sont responsables de la sécurité de l'accès aux données à caractère personnel.

Les administrateurs habilités « systèmes/réseau » gèrent les machines connectées au réseau de la HEAR ainsi que les serveurs sur lesquels sont

installés les différents services mis à la disposition des utilisateurs (services Internet, applications de gestion, services pour la recherche et la documentation).

Les enseignants habilités peuvent installer des logiciels adaptés à la pédagogie et la recherche au sein de leurs ateliers conformément aux conditions de commercialisation des éditeurs. Le téléchargement des sources logiciels devra se faire uniquement depuis le site de l'éditeur ou depuis les Store de confiance (Apple, Windows).

La définition des conditions d'accès et d'identification

L'utilisation des moyens informatiques de l'école a pour objet exclusif de réaliser des activités relevant des missions de l'établissement.

Chaque utilisateur se voit attribuer un compte informatique HEAR et un mot de passe l'habilitant à se connecter aux outils informatiques rattachés à ce compte. Par ailleurs, l'utilisateur peut se voir attribuer d'autres comptes affectés à des outils et services tiers. Les mêmes règles s'appliquent aux deux types de comptes.

Un compte informatique est strictement personnel et confidentiel. Chaque utilisateur est responsable de l'utilisation qui en est faite.

Le mot de passe provisoire du compte informatique HEAR transmis par le service informatique, puis celui choisi par l'utilisateur, doivent respecter les recommandations de la CNIL. Chaque utilisateur s'engage à personnaliser et à ne pas communiquer ce mot de passe à une tierce personne même à la demande de son supérieur hiérarchique.

Les conditions d'utilisation

Chaque utilisateur s'engage à prendre soin des matériels, des logiciels et des locaux informatiques mis à sa disposition.

Les comptes et identifiants des utilisateurs sont actifs tant qu'ils figurent dans les effectifs du personnel, des étudiants et tiers habilités (invités...).

Il est primordial que chaque utilisateur veille à ce que des tiers non autorisés ne puissent

accéder aux données de la HEAR. Les sessions informatiques ne doivent pas être accessibles en l'absence même ponctuelle des utilisateurs. Il convient donc de les verrouiller ou de se déconnecter ou d'arrêter l'ordinateur.

L'utilisateur doit s'efforcer de n'occuper que la quantité d'espace disque qui lui est strictement nécessaire et d'utiliser de façon optimale les moyens de compression des fichiers dont il



dispose.

Les activités risquant d'accaparer fortement les ressources informatiques (impression de gros documents, calculs importants, utilisation intensive du réseau) devront être réalisées aux moments qui pénalisent le moins l'école.

Il informera le responsable d'atelier ou le service informatique de toute anomalie constatée (pertes de données et d'intrusion...).

Chacun s'engage à respecter les règles de déontologie informatique qui impliquent, notamment, de ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- de masquer sa véritable identité
- d'utiliser le compte d'un autre utilisateur ;
- d'accéder sans habilitation à des données ou à des informations en vue de les altérer, de les détruire ou non ;
- de porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par

l'intermédiaire de messages, textes ou images provocants ou contraires à l'ordre public et aux bonnes mœurs ;

- de porter atteinte à l'intégrité du SI ou d'altérer le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau ;
- de désinstaller ou désactiver, de quelque manière que ce soit, les outils mis en place par le service informatique, notamment ceux destinés à la sécurité (antivirus, pare-feu, chiffrement, logiciel d'inventaire...) ;
- de se connecter ou d'essayer de se connecter sur un site internet sans y être autorisé ;
- de chercher à porter atteinte à des sites internet ;

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

Il informe le responsable d'atelier ou le service informatique de toute anomalie constatée.

Installation et utilisation de logiciels

L'utilisateur peut :

- installer un logiciel proposé à partir des plateformes mises en place par le service informatique (par exemple : « Self service ») ou des Store de confiance (Apple, Windows) ;
- demander l'installation de tout autre logiciel aux administrateurs selon leurs attributions.

L'utilisateur ne peut pas :

- faire une copie d'un logiciel commercial dont la licence appartient à la HEAR (par exemple : copie de la licence, clonage de l'ordinateur) ;
- contourner les restrictions d'utilisation d'un logiciel (par exemple : accéder à des services via des comptes génériques) ;
- développer des programmes qui s'auto-dupliquent ou s'attachent à d'autres programmes (virus informatiques) ;
- utiliser des copies de logiciels n'appartenant pas à la HEAR ;
- réaliser toute autre opération qui serait contraire à la présente charte.

Internet

Internet est un outil de travail ouvert aux usages relatifs aux missions de l'école. Son usage se fait dans le respect de la législation en vigueur.

En particulier, l'utilisateur :

- 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 administrateurs ;

— ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;

- ne doit pas usurper l'identité d'une autre personne et ne doit pas intercepter des communications entre tiers ;
- 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 ;
- ne doit pas déposer **des données sensibles à caractère personnel et/ou confidentiel** sur un serveur externe à la HEAR ou ouvert au grand public (Google, Free, Orange, ...) sans y être autorisé par les administrateurs ;
 - doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions... ;
 - doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire.
 - L'établissement ne peut pas être tenu pour responsable des violations de données et autres infractions commises par un utilisateur qui ne se sera pas conformé aux règles et lois en vigueur.
 - En dehors des usages liés à la pédagogie, à la recherche et aux services administratifs, l'utilisateur ne doit pas accaparer/saturer les ressources Internet par du téléchargement de documents lourds, de l'écoute de musique ou de radio, de visualisation de film sur Internet

A propos des torrents :

Ce sont des téléchargements de fichiers de type peer-to-peer (ordinateur à ordinateur). Indépendamment du caractère licite ou illicite, cette pratique peut aboutir à la saturation de la bande passante disponible au sein de la HEAR. Ces téléchargements sont par principe interdits à la

HEAR, sauf autorisation spécifique délivrée par les administrateurs habilités systèmes/réseau. Si des téléchargements de torrents sont constatés, l'utilisateur sera notifié et devra les arrêter. Si les téléchargements persistent, son compte Internet pourra être suspendu provisoirement sur décision de la direction.

A propos du filtrage de navigation :

Le contrôle par filtrage de la navigation exclut le contrôle des URL consultées. Toutefois, le pare-feu de la HEAR est équipé d'un dispositif de filtrage. Ce filtrage est basé sur une liste de catégories de sites fournie par l'Éducation nationale <https://www.data.gouv.fr/fr/datasets/liste-noire-durls/>.

Ainsi la HEAR bloque les catégories suivantes :

- Illegal : Sites presenting information (purchase, manufacture or required equipment) on illegal substances such as drugs
- Pornography : Sites with explicit sexual content. Includes adult products such as sex toys, CD-ROMs, and videos, adult services such as videoconferencing, escort services, and strip clubs, erotic stories and textual descriptions of sexual acts.
- Warez : Sites offering pirated software or which breach copyrights

Les dérogations à ce filtrage sont délivrées par la direction, et les administrateurs habilités systèmes/réseau qui opèrent sur demande écrite et motivée du responsable pédagogique et/ou de recherche

Messagerie électronique

La messagerie électronique est un outil de travail ouvert aux usages relatifs aux missions de l'école, dans le respect de la législation en vigueur.

- Tout message est considéré comme relatif aux missions de l'école, sauf s'il comporte une mention particulière et explicitée dans son objet indiquant son caractère privé ou s'il est stocké dans un espace privé de données (exemple : dossier nommé « personnel » ou « privé ») ;
- Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant

qu'éléments de preuve ;

- L'utilisateur doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages de masse ainsi que les encombrements inutiles et les dégradations du service ;
- Les mailing-listes seront utilisées à bon escient par les utilisateurs habilités ;
- Les messages groupés vers un nombre important de personnes doivent privilégier l'usage du cci (copie cachée) sauf besoin d'identification réciproque de l'ensemble des destinataires.



Mobilité et gestion des absences/départs

Les services scolarité et ressources humaines transmettent au service informatique les départs des étudiants et des agents/enseignants. Immédiatement après leurs départs, leurs habilitations (accès ou comptes informatiques) sont périmées et les agents/enseignants ne tentent plus d'y avoir recours, hormis requête de la HEAR dans une situation déterminée. Les accès informatiques (sessions serveur,

messagerie et différents services en ligne) seront désactivés après le départ de l'utilisateur.

Les accès à la messagerie seront conservés :

- 1 mois pour les agents et enseignants,
- 5 mois pour les étudiants.

Pour les agents en disponibilité pendant plus de 6 mois, leur messagerie sera conservée mais les listes auxquelles ils appartiennent seront expurgées jusqu'à leur retour.

Usage privé des moyens informatiques

Un usage privé des moyens informatiques est toléré dans la mesure où celui-ci est réalisé de bonne foi, de manière raisonnable et exceptionnelle, de sorte à ne pas perturber le fonctionnement du SI.

Les données collectées dans le cadre de cet usage peuvent contenir des données à caractère personnel concernant la vie domestique. A leur propos, afin de bénéficier de la protection de la vie privée en dehors des fonctions de l'utilisateur, elles doivent être stockées dans des espaces nommés « personnel » ou « privé » (stockage disque ou boîte mail).

Ainsi la HEAR considère que toutes les données collectées en dehors de ces espaces sont

strictement liées aux activités professionnelles de l'établissement et peuvent faire l'objet de mesures diverses d'administration (par exemple : accès lié à la continuité du service, suppression, déplacement, modification) si possible en informant l'utilisateur.

Les espaces personnels ou privés mis en place par l'utilisateur n'entrent pas dans la politique de sauvegarde de la HEAR et il lui appartient d'en garantir la conservation.

Le contrôle de ces zones de stockage « personnel ou privé » reste possible par la direction, selon des voies de droit. En cas de litige, les preuves en lien avec l'activité d'un agent dans sa zone de stockage privée peuvent être conservées.

Réseaux sociaux

L'évolution permanente des technologies de l'information met à disposition des utilisateurs de nouveaux services qui peuvent être accessibles depuis le réseau Internet. Ces nouvelles technologies, qui peuvent présenter un risque de vulnérabilité particulier, peuvent être limitées sur

décision de la direction de l'établissement et dans le strict respect de la politique de sécurité des systèmes d'informations. Actuellement, aucune politique de filtrage des réseaux sociaux n'a été mise en œuvre.

Sécurité

Des outils sont mis en place pour protéger les postes des utilisateurs contre les virus. Les logiciels antivirus sur les postes des utilisateurs sont paramétrés avec la stratégie suivante : en cas de détection d'un virus, le logiciel tente de réparer le fichier. Si la tentative échoue, le fichier est détruit. D'autres logiciels pourront être mis en place par le service Informatique pour protéger au mieux les données des utilisateurs et les

applications.

Les utilisateurs veillent à ne pas désactiver les outils mis en place par le service informatique (antivirus, pare-feu, chiffrement, logiciels d'inventaire...).



À propos de la traçabilité

L'ensemble des services utilisés génère, à l'occasion de leur emploi, « des fichiers de traces ». Ces fichiers sont essentiels à l'administration et la sécurité des systèmes. Ils servent en effet à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations telles que les horaires de connexion aux applications de gestion, au service de connexion à distance, le numéro de

l'ordinateur depuis lequel les services sont utilisés, etc. Ce type de traces existe pour l'ensemble des services, y compris Internet. Ces fichiers ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'un litige et après accord de la direction, ces fichiers peuvent être utilisés dans le cadre d'une procédure judiciaire. Les durées de conservation des logs et journaux sont conformes aux préconisations de la CNIL.

Contrôle et audit

Le service informatique peut, lorsqu'il constate un incident sur le SI (ex : manque de ressources lié à une activité inhabituelle), effectuer un contrôle sur les espaces utilisés ou accès Internet utilisés par les utilisateurs. Ce contrôle ne porte sur le

contenu des espaces mais leurs caractéristiques techniques (volumétrie, flux...). Il les informe dès que possible et prend les mesures nécessaires pour le rétablissement du fonctionnement du SI

Règles de conservation et de sauvegarde des données

Le service informatique, pour toutes les informations stockées dans les espaces réseaux, assure l'intégrité et la disponibilité des données dans la limite des moyens matériels. Les données stockées sur les serveurs administratifs et pédagogiques sont sauvegardées sur des serveurs distincts. Il ne pourra être tenu responsable de la perte de données en cas de panne de matériel. L'utilisateur doit effectuer des sauvegardes régulières de ses données stockées en local sur les ordinateurs (ex : bureau, répertoire Téléchargements).

Les ordinateurs pédagogiques, notamment ceux des salles informatiques, peuvent être formatés/ réinstallés chaque année pendant la pause estivale. Aussi il appartiendra aux utilisateurs, sous leur responsabilité, de récupérer/ sauvegarder leurs données locales avant le mois de juillet.

Les fichiers présents sur l'espace personnel serveur de l'utilisateur seront supprimés un mois après le départ de l'utilisateur.

Un rappel avertissant de la suppression future est délivré par le service informatique.

Prêt ponctuel de matériel

Le prêt de matériel est réglementé au sein de chaque atelier et par référence au règlement intérieur.

Concernant les prêts du service informatique, l'emprunteur signe un bordereau de prêt et reconnaît avoir emprunté les matériels y mentionnés. Il s'engage à les restituer dans le même état de fonctionnement, ou à prendre en charge tous les frais de réparation ou de remplacement du matériel correspondant au préjudice subi par la HEAR en cas de perte, vol ou détérioration.

L'emprunteur est responsable du matériel

emprunté et ce y compris dans les locaux de la HEAR.

S'il ne peut pas le surveiller, il conviendra par exemple de le sécuriser à l'aide d'un antivol ou cadenas.

Une assurance responsabilité civile est obligatoire. En cas de retards, la HEAR pourra relancer l'emprunteur par email, ou facultativement par SMS ou téléphone.



Matériel fourni par l'école aux agents

Le matériel fourni est soumis aux mêmes règles que celles décrites précédemment.

Un bordereau à signer pourra être demandé à

l'agent en cas de mise à disposition de matériel mobile (PC portable, smartphone, ...)

Sanctions et obligations particulières

Sanctions internes

L'accès illicite ou non conforme à la présente charte de la part d'un utilisateur peut entraîner la suppression de l'accès en toute ou partie aux

services numériques de la HEAR. Les fautes peuvent être sanctionnées disciplinairement.

Sanctions civiles

Les auteurs d'agissements contraires à la loi peuvent être condamnés à des réparations en dommages-intérêts aux victimes ayant subi des préjudices.

Sanctions pénales

La HEAR est tenue de signaler toute violation de la loi dûment constatée. Toute personne ayant connaissance d'un délit relatif au système d'information, aux traitements de données à caractère personnel et à la propriété intellectuelle,

est tenue d'en informer la direction. La direction pourra saisir la justice, si elle l'estime justifiée, dans les formes prévues par le Code de procédure pénale.

Propriété intellectuelle

L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, images, photographies ou autres créations protégés par

le droit d'auteur ou par un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.



Protection des données à caractère personnel

Dans l'accomplissement de son travail ou de ses missions, l'utilisateur est amené à collecter des données à caractère personnel.

Préalablement à tout traitement de données à caractère personnel, il est rappelé que le « règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant

la directive 95/46/CE (règlement général sur la protection des données)» et la loi « informatique et libertés » imposent à minima la mise en place :

- d'un registre,
- d'une information légale à destination des personnes concernées.

Il appartient à l'utilisateur de prendre contact avec notre délégué à la protection des données (dpo@hear.fr) ou avec le service informatique.

Entrée en vigueur

L'entrée en vigueur de la Charte informatique de la HEAR correspond à la date de notification de la délibération du Conseil d'administration du 13 juin 2024.

Je déclare avoir pris connaissance de la présente charte et m'engage à la respecter.

Date :
Nom prénom :

Signature :