Charte internet

CHARTE D'UTILISATION DE L'INTERNET, DES RESEAUX ET DES SERVICES MULTIMEDIA DANS L'ECOLE OU L'ETABLISSEMENT SCOLAIRE

Généralités

- La fourniture de services liés aux technologies de l'information et de la communication ne peut répondre qu'à **un objectif pédagogique et éducatif.**

- **Tous les élèves inscrits** peuvent bénéficier d'un accès aux ressources et services multimédias de l'établissement **après acceptation de cette Charte**. Pour les mineurs, la signature de la charte est subordonnée à l'accord des parents ou du représentant légal.

- L'établissement s'engage à **préparer les élèves**, les conseiller et les assister dans leur utilisation des services proposés.

- L'élève s'engage à **respecter la législation** en vigueur, et l'établissement est tenu d'en faire cesser toute violation.

- Rappel de la loi : 5* oute utilisation sans autorisation ou atteinte à l'image, toute information à caractère diffamatoire, injurieux, obscène, offensant, violent, pornographique, susceptible par nature de porter atteinte au respect de la personne humaine et de sa dignité ou d'inciter à la violence politique, raciste ou xénophobe, tout message présentant sous un jour favorable le banditisme, le vol , la haine ou tout acte qualifié de crime ou délit, ou de nature à inspirer ou à entretenir les préjugés ethniques ou discriminatoires, quel qu'en soit le support, tombent sous le coup d'une sanction civile et pénale.

- Les administrateurs de réseaux peuvent, **pour des raisons techniques mais aussi juridiques,** être amenés à analyser et contrôler l'utilisation des services. Ils se réservent, dans ce cadre, le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système.

- L'établissement s'efforce de **maintenir les services accessibles** en permanence, mais peut interrompre l'accès pour toutes raisons, notamment techniques, sans pouvoir être tenu pour responsable des conséquences de ces interruptions.

- L'élève s'engage à **ne pas perturber volontairement le fonctionnement des services**, et notamment à ne pas utiliser de programmes destinés à contourner la sécurité, ne pas introduire de programmes nuisibles (virus ou autres), ne pas modifier sans autorisation la configuration des machines.

- L'utilisateur s'engage à n'effectuer aucune **copie illicite** de logiciels commerciaux.

Accès à l'Internet

- L'accès aux ressources du Web a pour objet exclusif des recherches dans le cadre d'activités pédagogiques.

- Les élèves mineurs ne peuvent mener ces recherches qu'en **présence d'un adulte responsable.**

- Aucun système de filtrage n'étant parfait, l'établissement ne peut être tenu responsable de la non-validité des documents consultés.

- L'établissement se réserve la possibilité de contrôler les sites visités par les élèves pour leur éviter d'accéder à des sites illicites ou interdits aux mineurs, et de vérifier que l'utilisation des services reste conforme aux objectifs pédagogiques.

Messagerie

- L'élève s'engage à n'utiliser le service, et notamment les listes d'adresses, **que pour un objectif pédagogique et éducatif**. Il s'engage en particulier à ne pas stocker, émettre ou faire suivre des documents à caractère violent, pornographique, diffamatoire ou injurieux. Il s'engage à ne pas procéder à du harcèlement.
- L'élève s'engage à garder confidentiel son mot de passe et à ne pas s'approprier le mot de passe d'un autre utilisateur.

Publication de pages Web

Lors de la mise en place de pages Web sur un site d'établissement, les rédacteurs doivent garder à l'esprit que sont interdits et pénalement sanctionnés :

- le non-respect des **droits de la personne** (atteinte à la vie privée d'autrui, racisme, diffamation, injure)
- la **publication de photographie** sans avoir obtenu l'autorisation écrite de la personne représentée ou de son représentant légal si elle est mineure.
- le non-respect des **bonnes mœurs**, des **valeurs démocratiques** et du principe de **neutralité** du service public
- le non-respect de la **propriété intellectuelle et artistique** (droits d'auteurs)
- le non-respect de la **loi informatique et libertés** (traitement automatisé de données nominatives)

Réseau pédagogique local

- L'identifiant et le mot de passe d'un élève sont strictement **personnels et confidentiels** et il est responsable de leur conservation.
- L'élève ne doit pas masquer son identité sur le réseau local, ou usurper l'identité d'autrui en s'appropriant le mot de passe d'un autre utilisateur.
- L'utilisateur ne doit pas effectuer des activités accaparant les ressources informatiques et pénalisant la communauté (impression de gros documents, stockage de gros fichiers, encombrement des boîtes aux lettres électroniques…).
- Un site Web consultable seulement en Intranet est **soumis aux mêmes règles** que s'il était publié sur Internet.

Sanctions

La Charte ne se substituant pas au règlement intérieur de l'établissement, le non-respect des principes établis ou rappelés par la Charte pourra donner lieu à une limitation ou à une suppression de l'accès aux services, et aux sanctions disciplinaires prévues dans le règlement intérieur de l'établissement.

Le Principal, *L'élève,*

Les parents,

Avenant à la charte informatique

I / RESPECT DE LA LOI INFORMATIQUE ET LIBERTE

La loi du 6 janvier 1978 dite « LOI INFORMATIQUE ET LIBERTE » impose à toute entité qui constitue ou opère des traitements sur des fichiers comportant des données nominatives ou personnelles de s'acquitter d'une déclaration ou d'une demande d'avis auprès de la Commission Nationale Informatique et Libertés (CNIL).

Pour protéger l'intégrité du réseau informatique et maintenir la disponibilité du système d'information, le Département déploie et utilise des outils de surveillance réseau et des outils de gestion et de supervision de parc.

Ces outils génèrent des fichiers de « traces » qui font l'objet conformément aux obligations légales de déclarations auprès de la CNIL.

II / AUTHENTIFICATION, ACCES AU RESEAU INFORMATIQUE PEDAGOGIQUE ET GESTION DES « TRACES »

Chaque utilisateur dispose d'un compte composé d'un identifiant et d'un mot de passe. Ces informations sont placées sous la responsabilité de l'utilisateur une fois transmises par l'établissement. Elles sont confidentielles et non cessibles.

Tout utilisateur, dès lors où il se connecte au réseau fait l'objet obligatoirement d'une authentification.

S'il est membre de l'annuaire de l'établissement et qu'il se connecte à partir d'une machine référencée, il est automatiquement authentifié. A défaut l'authentification se fait par le biais d'un portail captif.

Chaque connexion fait l'objet d'une « trace » dans un fichier. Toutes les connexions vers Internet sont tracées et les informations suivantes sont collectées : site visité, date, heure, identification du matériel pour se connecter, identifiant de connexion.

Ces fichiers, conformément aux dispositions légales, sont conservés un an maximum et ne sont utilisés qu'à des fins techniques en cas d'incident ou sur demande des autorités dans le cadre d'une procédure judiciaire.

III / INFORMATIONS DES UTILISATEURS SUR LA GESTION DU RESEAU DES OUTILS DE SUPERVISION ET DE SURVEILLANCE

Le Département met en place des outils qui permettent de consolider l'administration, le contrôle et la supervision du réseau, des postes de travail et des utilisateurs.

• Contrôle et sécurisation des flux réseaux

Pour protéger l'intégrité et maintenir la disponibilité du réseau de l'établissement, les flux réseaux font l'objet d'un traitement opéré par la solution de sécurité mise en place par le Département.

Ce dispositif permet de prévenir les attaques, les intrusions et de se prémunir du transit de contenus illicites conformément aux dispositions légales.

A ce titre, les flux chiffrés constituent un point important et spécifique qui appelle une attention particulière.

Afin de garantir les précautions et obligations décrites ci-dessous en matière de protection du réseau, ***un déchiffrement de ces flux est effectué.***

Ces flux étant cryptés entre l'utilisateur et le réseau Internet, la seule possibilité de sécuriser et de contrôler les données est le déchiffrement. Ce mécanisme se fait dans le strict respect de le loi.

Aussi, les données issues des flux bancaires, de protections sociales, de santé et de messagerie (Gmail, Yahoo, Hotmail, laposte ...) ne sont pas déchiffrées et le secret des correspondances et le respect de la vie privée est maintenu (pour les autres flux qui sont déchiffrés, aucune trace n'est stockée ou archivée).

• **Contrôle, supervision des postes et des utilisateurs**

- La sécurisation et la supervision des postes

Les postes de travail connectés au réseau informatique pédagogique font l'objet d'une politique de sécurité (restrictions à des accès ou à des fonctionnalités) qui vise à prémunir le système d'information d'éventuelles perturbations ou interruptions.
Les matériels peuvent faire l'objet d'interventions sur site ou à distance lorsque les circonstances le permettent.

- La gestion des salles de classe et la supervision de l'utilisation des postes

Le Département met en place une solution unique de consolidation de l'administration des postes de travail et de supervision de la gestion des salles de classes et de l'utilisation des postes.
Cet outil permet dans une console centrale, accessible uniquement à partir du poste professeur de chaque salle de classe, une visibilité et une surveillance en temps réel sur l'ordinateur ou la tablette de chaque utilisateur. Seule l'activité des élèves, matérialisée par des vignettes, est visible. Les postes professeurs ne sont pas observables.
Cet outil permet de mettre en place des blocages et des restrictions à des fins techniques ou pédagogiques.
Cet outil produit des fichiers de « traces » qui font l'objet d'une déclaration auprès de la CNIL.