Charte informatique de l'EPLEFPA Chartres – La Saussaye

Vu la loi du 11 Mars 1957
Vu la loi n° 78-153 du 5 Janvier 1978
Vu la loi n° 78-17 du 6 Janvier 1978
Vu la loi n° 85.660 du 3 Juillet 1985
Vu la loi n° 88-19 du 5 Janvier 1988
Vu la loi n° 91-646 du 10 juillet 1991
Vu la loi n° 92-597 du 1er Juillet 1992
Vu la loi n° 2004-575 du 21 Juin 2004
Vu la loi n° 2004-801 du 6 août 2004
Vu la circulaire SG/SM/SDSI/MSSI/C2007-1402 CAB/MD/C2007-0001 du 10 février 2007
Vu la circulaire SG/SM/N2007-1408 CAB/MD/N2007-0007 du 01 août 2007
Vu la loi n° 2009-1311 du 28 octobre 2009
Vu L'article 9 du Code civil
Vu l'arrêté du 6 mai 2010

1. Pourquoi une charte ?

L'objectif premier de la charte est de présenter les quelques règles simples mais essentielles de bonne utilisation des ressources informatiques de l'EPLEFPA. Ces règles relèvent avant tout du bon sens et cherchent à garantir à chacun l'utilisation optimale de ces ressources, ainsi que leur sécurité.
La charte doit également informer les utilisateurs de la législation en vigueur. Elle est un contrat entre l'utilisateur désireux d'accéder aux ressources informatiques et le directeur l'EPLEFPA. Chaque utilisateur devra donc signer l'accusé de réception mentionnant qu'il a pris connaissance de cette charte et qu'il s'engage à en respecter les termes.
Tout d'abord, il convient de définir les termes suivants :

- Ressources informatiques : tout matériel informatique, logiciels, service de communication numérique et ressources externes (par exemple Internet)
- Utilisateur: toute personne, quel que soit son statut (enseignant, formateur, apprenant, technicien, administratif, personnel temporaire, stagiaire, etc.) appelée à utiliser les ressources informatiques et réseaux de l'établissement
- Administrateur: la gestion des ressources est assurée par un ou plusieurs membres du personnel permanent de l'EPLEFPA. Ils sont appelés administrateurs et sont chargés de la mise en œuvre des mesures de sécurité des systèmes d'information

2. Conditions générales d'utilisation

- L'utilisation des moyens informatiques est limitée au strict cadre et aux seuls besoins des activités et de la vie de l'EPLEFPA.
- Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.
- Toute autre utilisation des moyens informatiques doit être préalablement autorisée par le directeur de l'EPLEFPA.
- Sont strictement prohibées les utilisations contraires aux lois et règlements en vigueur (voire annexe 1) et notamment celles qui sont de nature à porter atteinte aux bonnes mœurs, à la dignité, à l'honneur, ou à la vie privée des personnes.

3. Obligations des utilisateurs

3.1. Régles générales

Tout utilisateur :

- est tenu de respecter les matériels, logiciels et locaux mis à sa disposition.
- se doit de veiller à ne pas modifier les raccordements des matériels aux réseaux de communication interne et externes
- s'engage à ne pas connecter un matériel personnel ou extérieur à l'établissement sur le réseau sans autorisation du directeur de l'EPLEFPA.
- s'engage à ne pas installer de logiciels sans l'accord de l'administrateur et à ne pas utiliser de logiciels sans en avoir préalablement acquis la licence.
- qui constate une dégradation ou un dysfonctionnement doit, dans les plus brefs délais, informer l'administrateur de l'établissement.

Plus généralement, aucune modification des environnements logiciels, matériels et périphériques ne pourra être effectuée sans l'accord préalable du directeur de l'EPLEFPA. Par modification d'environnement on entend toute suppression ou ajout de composants logiciels ou matériels ou tout paramétrage pouvant affecter le fonctionnement normal des moyens informatiques.
L'introduction, l'utilisation, la diffusion de tout dispositif logiciel ou matériel qui pourraient altérer les fonctionnalités des moyens informatiques sont interdites.

3.2. Utilisation des comptes et des dispositifs de contrôle d'accès.

Les utilisateurs sont responsables de l'utilisation qu'ils font des ressources informatiques et des matériels mis à leur disposition, et à ce titre ils doivent notamment :

- veiller à la confidentialité des codes, mots de passe, cartes magnétiques, clefs ou tout autre dispositif de contrôle d'accès qui leur sont confiés à titre strictement personnel.
- choisir un mot de passe sûr et gardé secret, y compris vis-à-vis des administrateurs.
- veiller à la confidentialité des comptes utilisateurs qui leur sont attribués à titre strictement personnel.
- ne pas prêter, vendre ou céder les comptes utilisateurs, codes et autres dispositifs de contrôle d'accès ou en faire bénéficier un tiers.
- se déconnecter immédiatement après la fin de leur période de travail sur le réseau ou lorsqu'ils s'absentent.
- S'abstenir de toute tentative d'appropriation ou de déchiffrage du mot de passe d'un autre utilisateur.
- informer immédiatement l'administrateur de l'établissement de toute tentative d'accès frauduleux ou de tout dysfonctionnement suspect.
- s'assurer que les fichiers qu'ils jugent confidentiels ne soient pas accessibles à des tiers.

Pour rappel un utilisateur est responsable de la confidentialité et de la sécurité de ses identifiants. En cas de prêt, perte ou vol, l'utilisateur pourrait être tenu responsable de tout agissement (vol et consultation de documents, téléchargement illégal, consultation de site internet prohibé …) commis à l'aide de ceux-ci.

4. Charte éditoriale

Cet article s'impose à tout personnel ou apprenant souhaitant publier des informations ou des documents sur les sites de l'EPLEFPA.
L'usage du droit de publication devra respecter toute réglementation applicable dans ce domaine :

- respect des droits d'auteurs, du régime juridique des licences publiques et de la législation liés aux documents écrits et audiovisuels : chaque auteur devra s'assurer qu'il a le droit de diffuser les documents qu'il propose.
- l'article L 122-5 du code de la propriété intellectuelle n'autorisant que les " copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective " et " les analyses et les courtes citations dans un but d'exemple et d'illustration ", toute représentation ou reproduction intégrale ou partielle faite sans consentement de l'auteur est interdite, les citations devront êtres courtes et leur source clairement indiquée

- respect du droit à l'image : il convient de vérifier que les images sont bien libres de droits ou d'obtenir une autorisation écrite du détenteur de ces droits
- conformément à l'article 34 de la loi " Informatique et Libertés " du 6 janvier 1978, les personnes citées disposent d'un droit d'accès, de modification, de rectification et de suppression des données qui les concernent.

Le contenu des informations publiées sur les sites de l'EPLEFPA doit respecter certaines règles :

- respect du service public
- pas de publicité commerciale, en dehors de celle en lien avec l'ALESA ou l'exploitation agricole de l'EPLEFPA. Les citations d'entreprises sont autorisées, si elles ne revêtent pas un caractère commercial

5. Développement durable

Par l'intermédiaire de cette chartre, l'EPLEFPA souhaite sensibiliser chaque utilisateur à adopter un comportement « éco-citoyen », lorsqu'il utilise les ressources de l'établissement.
Il est demandé :

- d'éteindre son poste de travail (unité centrale, écran, imprimante …) à la fin de son activité , la mise en veille d'un équipement ne stoppant pas complètement sa consommation d'énergie.
- d'avoir une réflexion sur les impressions : « Eviter les impressions inutiles », « réutiliser d'anciennes feuilles de papier quand cela est possible », « favoriser le recto verso » sont des gestes simples à adopter.

6. Rôle de l'administrateur

Les ressources informatiques de l'EPLEFPA sont administrées par le TEPETA informatique (administrateur), qui s'engage à prendre toute disposition utile pour permettre le bon fonctionnement des ressources informatiques communes. De ce fait, il :

- autorise les accès aux moyens informatiques.
- attribue les comptes et les mots de passe ou tout autre dispositif permettant l'accès aux moyens informatiques conformément à la politique de l'établissement.
- assure le fonctionnement et la disponibilité normale des moyens informatiques.
- s'assure de la sécurité du système d'information.

Pour des nécessités de maintenance, de gestion technique, ou réglementaire, l'administrateur s'engage à :

- analyser et contrôler l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau, dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.
- surveiller en détail les sessions de travail d'un utilisateur soupçonné de non-respect de la charte. Dans ce cas, il devra en informer le directeur de l'EPLEFPA.
- prendre les dispositions nécessaires à l'encontre d'un utilisateur ou d'un matériel informatique qui gênerait le bon fonctionnement des ressources informatiques.
- effacer ou comprimer, les fichiers excessifs ou sans lien direct avec une utilisation normale du système informatique.

Devoir de l'administrateur :

- L'administrateur ne peut accéder à des fichiers ou des courriers privés que pour des activités de diagnostic ou de correction de problème. Il ne peut examiner les données des utilisateurs que pour la bonne marche des systèmes ou la vérification du non respect de la charte.
- L'administrateur doit respecter la confidentialité des fichiers utilisateurs, des courriers et des sorties imprimantes auxquels ils peuvent être amenés à accéder.
- L'administrateur doit informer les utilisateurs des interruptions volontaires de service. Il doit minimiser celles-ci et choisir, si possible, les dates les moins pénalisantes pour les utilisateurs.

7. Conséquences des manquements à la charte et poursuites

7.1. Mesures applicables par les responsables informatiques

7.1.1. Mesures d'urgence

L'administrateur peut en cas d'urgence :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation
- isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques

7.1.2. Mesures donnant lieu à information

Sous réserve que soit informé le directeur, le personnel de l'EPLEFPA peut :

- avertir un utilisateur
- limiter provisoirement les accès d'un utilisateur
- à titre provisoire, retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes
- effacer, comprimer ou isoler toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril le fonctionnement des moyens informatiques

7.1.3. Mesures soumises à autorisation du directeur ou responsable du service

Sous condition d'autorisation préalable du directeur de l'EPLEFPA, l'administrateur peut :

- retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes
- interdire à titre définitif à un utilisateur tout accès aux moyens informatiques dont il est responsable

7.1.4. Sanctions disciplinaires

Les utilisateurs ne respectant pas les règles et les obligations de la charte sont également passibles d'une procédure disciplinaire inhérente à leurs statuts.

7.1.5. Poursuites civiles et pénales.

Tout utilisateur qui contreviendrait aux règles précédemment définies peut s'exposer à des poursuites civiles et/ou pénales prévues par les textes en vigueur (articles 323-1 à 323-7 du code pénal).

8. Cas particuliers

8.1. Salle accès libre BTS.

Une salle libre accès destinée aux activités pédagogiques permet aux étudiants de BTS de connecter leurs ordinateurs personnels au réseau de l'établissement.
En utilisant cette salle l'étudiant, s'engage à :

- respecter l'article 2, 3.1, 3.3 et 4 de cette charte
- limiter ses activités aux besoins liés à sa scolarité
- prévenir l'administration de l'EPLEFPA, s'il constate qu'un utilisateur ne respecte pas les règles de ce lieu de travail.

En utilisant cette salle l'étudiant reconnait:

- que la salle libre accès n'étant pas surveillée physiquement par un personnel de l'établissement, l'administrateur vérifiera spécialement l'activité internet de ces utilisateurs. Les sanctions prévues par l'article 6 pourront être appliquées et une fermeture de la salle pourra être mise en place en cas de violation de la charte.
- qu'une salle spécifique lui étant attribué pour pouvoir étudier, il renoncera à brancher son ordinateur personnel sur le réseau informatique de l'établissement, hors de cette salle.
- que l'EPLEFPA ne peut être tenu responsable d'un disfonctionnement de son matériel personnel lors d'une connexion au réseau informatique de l'établissement.

8.2. Connexion de personne extérieure sur le réseau de l'établissement

Toute personne extérieure à l'établissement (intervenant, technicien chargé de maintenance, technicien hotline, commercial…) doit demander une autorisation à l'administrateur pour se connecter au réseau informatique de l'établissement. Cette connexion, si elle n'est pas jugée à risque, sera autorisée sur des prises spécifiques et se limitera à l'accès d'internet suite à une identification.
Aucun utilisateur n'est habilité à faciliter la connexion d'une personne extérieure à l'EPLEFPA.
Il est formellement interdit d'autoriser une prise en main à distance, sans l'accord et la présence d'un administrateur.

8.3. Formation et pratique spécifique nécessitant des droits étendus.

Lorsqu'une formation et ou une pratique nécessite des droits utilisateurs étendus (droits administrateur local par exemple), une demande justifiée devra être faite au directeur de l'EPL, qui donnera suite en accord avec l'administrateur.
Toute pratique nécessitant des droits « administrateur local », entrainera une isolation du système d'information de l'établissement.
Pour des raisons de sécurités évidentes, aucun droit administrateur du domaine ne sera délivré en dehors du service informatique.

8.4 Prêt de matériel

Pour des raisons de sécurité et dans l'impossibilité de garantir l'intégrité d'un réseau local extérieur à l'établissement, Il est formellement interdit de brancher le matériel de prêt sur quelques réseaux extérieurs que ce soit (domicile entreprise…)

Annexe 1 : Guide juridique

Les références ci-dessous font appel à divers textes de loi venant de différents codes. Il est important de connaître ces bases sur lesquels les juristes s'appuient. Les fortes modifications dans ce secteur doivent amener chacun à ne pas considérer seulement ces textes mais également et plus particulièrement à suivre les différentes jurisprudences en cours. Les textes de loi étant pour certains relativement larges, les jugements rendus sont des interprétations qui donnent un éclairage plus précis de l'application des différents textes.

A. Protection des systèmes d'information et fraude informatique.

Le texte de référence est la loi 88-19 du 5 janvier 1988 (loi Godefrain) reprise dans le code pénal aux articles 323-1 à 323-7. Sont considérées et punies comme des délits les activités suivantes :

- Accès illicite[1] ou maintien frauduleux[2] dans un système informatique
- Atteinte volontaire au fonctionnement d'un système informatique[3]
- La tentative de ces délits
- L'association en vue de les commettre.

Par ailleurs, la création de faux et leur usage, constitue un délit autonome sanctionné au titre de faux en écriture privée, publique ou de commerce.

B. Responsabilité en matière de transmission des informations

Les moyens informatiques mis à disposition de l'utilisateur ne doivent pas permettre de véhiculer n'importe quelle information ou donnée mettant en cause des mineurs (articles 227-23 du Code pénal).
L'article 227-24 du Code pénal précise que le fait, soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.

C. Cryptologie.

Conformément à la réglementation en vigueur et en particulier aux modalités fixées par les décrets 99-199 et 99-200 du 17 mars 1999, les logiciels de cryptologie disponibles en téléchargement sur l'Internet peuvent être utilisés librement dés lors que ceux-ci ont fait l'objet d'une déclaration ou bénéficient d'une autorisation de fourniture préalable.

D. Protection des données à caractère personnel et des personnes

Les données à caractère personnel font l'objet d'une protection légale particulière dont la violation expose son auteur à des sanctions pénales.
Les textes applicables en la matière sont les suivants :

- loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 aout 2004
- la convention n°108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.
- La directive n°95/46 du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[1] Article 323-1 du Code pénal
[2] Article 323-3 du Code pénal
[3] Article 323-2 du Code pénal

E. Messagerie électronique

Secret des correspondances

La loi n°91-646 du 10 juillet 1991 sur le secret des correspondances stipule que le secret des correspondances par la voie des communications électroniques est garanti par la loi.
Seules les interceptions dites de sécurité ou ordonnées par l'autorité judiciaire sont autorisées dans un cadre défini et contraint.
L'article 226-15 du Code pénal stipule qu'est puni d'un an d'emprisonnement et de 45000 euros le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination adressées à des tiers, ou d'en prendre frauduleusement connaissance, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises ou transmises par la voie de télécommunication ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.
L'article 432-9 du code pénale stipule que le fait de faire la même chose par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice de ses fonctions est puni de trois ans d'emprisonnement et de 45000 euros d'amende.

Preuve

Le principe est celui de la liberté de la preuve qui peut être apportée par tout moyen, ainsi, un message électronique peut constituer une preuve susceptible d'engager la responsabilité de l'institution ainsi que celle de l'expéditeur (article 1316-1 à 4 du Code civil).

F. Protection des droits de propriété intellectuelle

Protection des logiciels.

Le titre 5 de la loi du 11 mars 1957, complété par la loi 85-660 du 3 juillet 1985 et par la circulaire du 17 octobre 1990, relative aux droits d'auteurs et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes, et des entreprises de communication audiovisuelle, s'applique aux droits d'auteurs de logiciels informatiques.
Toute copie de logiciel protégé est interdite et s'apparente à du vol.
Aucun code source d'un logiciel protégé ne peut être inclus dans des logiciels pouvant être utilisés à l'extérieur.
La licence d'utilisation de certains logiciels restreint parfois l'utilisation de ceux-ci à des fins pédagogiques : l'utilisateur doit donc se renseigner avant d'utiliser un logiciel pour la recherche ou la gestion.

Protection du droit d'auteur

En vertu des règles du Code de la propriété intellectuelle, l'auteur d'une œuvre d'esprit jouit sur cette œuvre du seul fait de sa création « d'un droit de propriété incorporel et exclusif opposable à tous ».
Cette disposition s'applique à toutes les œuvres de l'esprit quel qu'en soit le genre, la forme d'expression, le mérite ou la destination.
On y retrouve donc : les livres, brochures, écrits divers, œuvres dramatiques, chorégraphiques, musicales, graphiques, photographiques, etc.

Prévenir le téléchargement et de mise à disposition illicite d'œuvres

L'article 336-3 du Code de la propriété intellectuelle stipule que : « La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. »

Protection des données et des bases de données.

La protection des droits d'auteurs s'étend donc aux données telles que les textes, images et sons et leur utilisation ne doit se faire qu'avec l'autorisation du titulaire des droits. La plus grande prudence doit être de

mise pour des sources venant d'Internet ou la connaissance du titulaire des droits peut s'avérer difficile, voir impossible.
Les bases de données qui, par le choix ou les dispositions des matières, constituent des créations intellectuelles bénéficient des dispositions du Code de la propriété intellectuelle.

G. Protection des marques

Le Code de la propriété intellectuelle protège dans son article 711-1 « toute marque de fabrique, de commerce ou de service servant à distinguer les produits ou services d'une personne physique ou morale ».

H. Respect de la vie privée

Droit à la vie privée

L'article 9 du Code civil prévoit que « chacun a droit au respect de sa vie privée ».
Il cite également : « Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée ».

Droit à l'image

L'article 226-1 du Code pénal préserve le droit à l'image de l'individu :
« Est puni d'un an d'emprisonnement et de 45000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :
En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. »
L'article 226-2 qu'il est puni de la même peine le fait de « conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1. »

Droit de représentation

L'article 226-8 du Code pénal stipule « Est puni d'un an d'emprisonnement et de 15000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention. »

I. Obligation d'information

« Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. » (Article 40 du Code de procédure pénale)

J. Informations sensibles ou classifiées.

IGI[4] 900 du 20 juillet 1993 pour le classifié.
IGI 901 du 20 juillet 1993 pour le sensible.

[4] IGI : Instruction Générale Interministérielle