



Charte de bon usage de l'informatique et des réseaux du lycée G.Eiffel de Talange

(Charte validée par le Conseil d'Administration, le 14 Décembre 2000)

La présente charte a pour objet de définir les règles d'utilisation des moyens et systèmes informatiques des lycées LP et LT G.EIFFEL de Talange. Elle est annexée au règlement interne de l'établissement par décision du CA du 14 Décembre 2000. Elle s'inscrit dans le cadre des lois en vigueur :

- Loi n° 78-17 du 6 janvier 1978 "informatique, fichiers et libertés"
- Loi n° 78-753 du 17 juillet 1978 sur l'accès aux documents administratifs,
- Loi n° 85.660 du 3 juillet 1985 sur la protection des logiciels,
- Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique,
- Loi n° 92-597 du 1er juillet 1992 (code de la propriété intellectuelle).

1. CHAMP D'APPLICATION DE LA CHARTE :

Les règles et obligations ci-dessous énoncées s'appliquent à toute personne : élèves, enseignants, stagiaires, personnels administratifs ou techniques, autorisée à utiliser les moyens et systèmes informatiques du lycée Eiffel

Ces derniers comprennent notamment les réseaux, serveurs, stations de travail et micro-ordinateurs. . Le respect des règles définies par la présente charte s'étend également à l'utilisation des systèmes informatiques d'organismes extérieurs au lycée, accessibles par l'intermédiaire d'Internet.

2. CONDITIONS D'ACCES AUX MOYENS INFORMATIQUES DU LYCEE :

L'utilisation des moyens informatiques du lycée a pour objet exclusif de mener des activités d'enseignement ou de documentation. Ces moyens ne peuvent être utilisés en vue de réaliser des projets ne relevant pas des missions confiées aux utilisateurs.

Chaque utilisateur d'un réseau se voit attribuer un compte informatique par un administrateur. Les comptes et mots de passe sont inaccessibles. Les comptes nominatifs sont personnels. Chaque utilisateur est responsable de l'utilisation qui en est faite.

L'utilisateur prévient l'administrateur si son mot de passe ne lui permet plus de se connecter ou s'il soupçonne que son compte est violé.

3. LE RESPECT DE LA DEONTOLOGIE INFORMATIQUE :

3.1 REGLES DE BASE : Chaque utilisateur s'engage à respecter les règles de la déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- de masquer sa véritable identité ;
- de s'approprier le mot de passe d'un autre utilisateur ;
- de modifier ou de détruire des informations ne lui appartenant pas sur un des systèmes informatiques ;

• d'accéder à des informations appartenant à d'autres utilisateurs sans leur autorisation ;

• de porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants ;

- d'interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés ou non au

réseau ;

- de se connecter ou d'essayer de se connecter sur un site sans y être autorisé.
- la création de tout fichier contenant des informations nominatives doit faire l'objet d'une demande préalable auprès de la Commission Nationale de l'Informatique et des Libertés

La réalisation ou l'utilisation d'un programme informatique ayant de tels objectifs est strictement interdite.

3.2 UTILISATION DE LOGICIELS ET RESPECT DES DROITS DE LA PROPRIETE : L'utilisateur ne peut installer un logiciel sur un ordinateur ou le rendre accessible sur le réseau qu'après avis du ou des administrateurs concernés.

L'utilisateur s'interdit de faire des copies de logiciels n'appartenant pas au domaine public.

Notamment, il ne devra en aucun cas :

- installer des logiciels à caractère ludique sauf à des fins scientifiques ou pédagogiques ;
- faire une copie des logiciels commerciaux pour lesquels le lycée a acheté les licences, et qu'il a installés sur le réseau
- contourner les restrictions d'utilisation d'un logiciel ;
- développer des programmes qui s'auto-dupliquent ou s'attachent à d'autres programmes (virus informatiques).

3.3 UTILISATION EQUITABLE DES MOYENS INFORMATIQUES : Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il informe le responsable du matériel informatique de toute anomalie constatée.

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 utilisateurs doivent périodiquement effectuer des sauvegardes de leurs données (sur disquettes, ...)

Il respecte les principes d'économie des consommables.

- L'informatique au lycée en salle de cours est un instrument de travail

L'informatique peut avoir une multitude d'applications, mais, au lycée elle est un outil de travail (moyen d'information, de formation, de communication) et non un substitut aux consoles de jeux vidéos. L'utilisation et encore plus l'installation de jeux sont donc totalement interdits.

- Utilisation des imprimantes.

L'impression d'un document ne se fait qu'avec l'accord et sous le contrôle d'un enseignant. Les utilisateurs doivent contrôler l'impression de leurs documents sur les ordinateurs pilotant leur imprimante. Elle doit toujours être précédée d'un aperçu avant impression pour éviter les tirages inutiles.

Il est totalement interdit d'imprimer plusieurs exemplaires du même document. Si cela est nécessaire, il faut recourir à la photocopieuse dont le prix de revient est environ quatre fois inférieur.

- Respect des locaux, du matériel et des procédures d'utilisation.

Le matériel informatique est fragile, il faut donc le manipuler avec précaution et en respectant des procédures.

Par exemple :

- « fermer » correctement les logiciels que l'on utilise,
- déconnecter l'ordinateur du réseau ou lorsqu'on a fini de travailler, ne pas l'éteindre inutilement,
- ne pas manger, fumer, utiliser de la craie, ni boire dans une salle informatique,
- signaler tout problème rencontré à un professeur
- ne pas débrancher de périphérique sans autorisation,
- laisser sur place les tapis de souris

Il est interdit, sauf pour les besoins de maintenance et par les personnes désignées, de déplacer un moniteur ou une unité centrale, même par simple glissement sur le bureau support.

- Utilisation d'Internet :

L'utilisateur s'engage à ne visionner ou diffuser aucun document à caractère raciste, xénophobe ou pornographique. Tout site découvert en naviguant et dont le contenu est contraire à la loi devra être signalé au chef d'établissement. En salle de cours, l'utilisateur s'engage à ne consulter Internet que pour la recherche qu'il a précisée ou qui a été fixée par l'enseignant.

4 Sanctions encourues en cas de non-respect des règles éditées dans la présente charte

L'utilisateur qui ne respectera pas ces règles sera soumis aux sanctions suivantes :

disciplinaires : progressivement, et en fonction de la gravité des faits

- Un avertissement de l'utilisateur concerné.
- La réduction des droits de l'utilisateur sur le réseau (limitation de l'espace disque, de l'accès à certains logiciels)
- La suppression du «compte» personnel de l'utilisateur sur le réseau.
- L'interdiction totale de l'utilisation du matériel informatique.

civiles et/ou pénales : Les lois et textes réglementaires cités au début de cette charte, définissent les droits et obligations des personnes utilisant les moyens informatiques. Tout utilisateur n'ayant pas respecté ces lois peut être poursuivi pénalement.

Cette charte, partie intégrante du règlement intérieur du lycée Eiffel est portée à la connaissance de l'ensemble du personnel et s'impose à tous.

#-----

Je soussigné,

Nom Prénom

utilisateur des moyens informatiques et réseaux du lycée Eiffel déclare avoir pris connaissance de la présente charte de bon usage de l'informatique et des réseaux au lycée Eiffel.

Lu et approuvé le : / / 2001

Nous mettons à la disposition, et invitons tous nos utilisateurs à lire attentivement la loi GODFRAIN, loi du 5 janvier 1988 relative à la fraude informatique.

Loi numéro 88-19 du 5 janvier 1988 relative à la fraude informatique ou loi GODFRAIN

La loi du 5 janvier 1988 ou loi GODFRAIN est constituée des articles suivants :

- **Art 462-2 alinéa 1er** : délit d'intrusion dans le système d'autrui
- **Art 462-2 alinéa 2** : délit d'intrusion ayant entraîné des dégradations involontaires
- **Art 462-3** : délit d'entrave au système
- **Art 462-4** : délit d'atteinte aux données
- **Art 462-5** : faux informatique
- **Art 462-6** : usage de documents informatisés falsifiés
- **Art 462-7** : tentatives des délits
- **Art 462-8** : participation à une association délictueuse
- **Art 462-9** : confiscation des matériels

1) Art 462-2 alinéa 1er : délit d'intrusion dans le système d'autrui

1.1 Art 462-2 alinéa 1er : "Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de 2 mois à un an et d'une amende de 2 000 F à 50 000 F ou de l'une de ces 2 peines seulement."

1.2 système informatique :L'accès indu et le maintien indu dans un système informatique sont incriminés. L'accès non autorisé dans le système est donc réprimé, alors même qu'il n'en ait résulté aucun préjudice. Le seul fait d'entrer dans le système sans qu'il y ait lieu à considérer le but poursuivi ou les conséquences possibles, est incriminable en temps que tel. Le maintien non autorisé dans un système, même de manière parfaitement inoffensive est incriminable. La personne poursuivie doit avoir pénétré le système ou s'être maintenu dans celui-ci sans y avoir droit. Non respect des conditions d'accès au système

ou de maintien dans celui-ci.

1.3 La personne ou élément moral : Il s'agit d'un délit volontaire puisque l'accès et le maintien dans le système doivent avoir été accomplis frauduleusement. L'auteur ou les auteurs doivent avoir conscience de l'irrégularité de leur acte. Le maintien volontaire dans un système d'autrui est incriminable.

1.4 Exemples : - Piratage d'un compte d'un autre utilisateur en utilisant un faux login
- Tentative de connexion dans un système en utilisant toutes les combinaisons possibles de login et de mots de passe.
- Recherche d'informations afin de contourner les mécanismes de sécurité (parcours d'une hiérarchie système ou utilisateur).

2) Art 462-2 alinéa 2 : délit d'intrusion ayant entraîné des dégradations involontaires

2.1 Art 462-2 alinéa 2 du code pénal : "Lorsque il sera résulte (de l'intrusion ou du maintien non autorise dans le système) soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de 2 mois à 2 ans et l'amende de 10 000 F à 100 000 F."

2.2 Le système informatique : La dégradation du système commise suite à l'accès non autorise ou au maintien indu dans le système constitue l'élément matériel de l'infraction.

2.3 Exemples : Écriture de programmes , stockage de données ou modification de paramètres système ou réseau.

3) Art 462-3 : délit d'entrave au système

3.1 Art 462-3 : "Quiconque aura, intentionnellement et au mépris des droits d'autrui, entrave ou fausse le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de 3 mois à 3 ans et d'une amende de 10 000 F à 100 000 F ou de l'une de ces 2 peines."

3.2 Le système informatique :

- L'entrave, consiste à ralentir ou paralyser un système informatique. Saturer un système de fichiers volontairement. Outrepasser la convention d'utilisation du système.
- Fausser, c'est ce qui fait produire au système un résultat autre que celui attendu. C'est le cas par exemple de virus, de bombes logiques, de fausses commandes ...

4) Art 462-4 : délit d'atteinte aux données

4.1 Art 462-4 : "Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient, ou leur mode de traitement ou de transmission, sera puni d'un emprisonnement de 3 mois à 3 ans et d'une amende de 2000 F à 500 000 F ou de l'une de ces 2 peines."

4.2 Le système informatique : Il s'agit de l'introduction, de la modification ou de la suppression de données.

4.3 Exemples : Tentative d'écriture, de modification ou de suppression de données, de fichiers, ou de répertoires dans un autre environnement que le votre...

5) Art 462-5 : faux informatique

5.1 Art 462-5 : "Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à 5 ans et d'une amende de 20 000 F à 2 000 000 F."

5.2 Le système informatique : Altération de l'information traitée par le système (fausses commandes ...)

6) Art 462-6 : usage de documents informatisés falsifiés

6.1 Art 462-6 : "Quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à 5 ans et d'une amende de 20 000 F à 2 000 000 F ou de l'une de ces 2 peines seulement."

6.2 Le système informatique : Utilisation de l'altération de l'information (utilisation de fausses commandes ...)

7) Art 462-7 : tentatives des délits

7.1 Art 462-7 : "La tentative des délits prévus par les articles 462-2 à 462-6 est puni des mêmes peines que le délit lui-même."

8) Art 462-8 : participation à une association délictueuse

8.1 Art 462-8 : "Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou plusieurs infractions prévues par les articles 462-2 à 462-6 du code pénal sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée"

8.2 Le système informatique : Ce n'est pas forcément une association de la loi de 1901, il peut s'agir d'un groupement quelconque, voire une simple réunion dans le but de commettre des fraudes informatiques.

8.3 Exemple : Se passer des noms de login et des mots de passe de comptes déjà piratés

9) Art 462-9 : confiscation des matériels

9.1 Art 462-9 : "Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre."

[Aller au début](#)

[Recherche étendue](#) | [Carte des salles](#) | [Notifier](#) | [Télécharger](#) | [Imprimer](#) | [Aide](#)