CHARTE INFORMATIQUE
DES ELEVES, ETUDIANTS ET STAGIAIRES
COLLEGE, LYCEE, ENSEIGNEMENT SUPERIEUR ORT LYON

I/ CHAMP D'APPLICATION DE LA CHARTE

Les règles et obligations ci-dessous énoncées s'appliquent à toute personne ; en particulier enseignants, formateurs, étudiants, stagiaires, élèves et membres du personnel administratif ou technique ; autorisée à utiliser les moyens et systèmes informatiques de l'établissement ORT LYON. Ces derniers comprennent notamment les serveurs, stations de travail, micro-ordinateurs et imprimantes des services administratifs, des salles de cours ou d'informatique, et du centre de documentation. Le respect des règles définies par la présente charte s'étend également à l'utilisation des systèmes informatiques d'organismes extérieurs à l'établissement, systèmes accessibles par l'intermédiaire des réseaux de l'établissement, par exemple le réseau Internet. Toute personne qui valide son inscription à l'établissement ORT signe implicitement l'acceptation des termes de la présente charte.

II/ CONDITIONS D'ACCES AUX RESEAUX INFORMATIQUES DE L'ETABLISSEMENT

L'utilisation des moyens informatiques de l'établissement a pour objet exclusif de mener des activités de recherche, d'enseignement ou d'administration. Sauf autorisation préalable délivrée par le service informatique, ces moyens ne peuvent être employés en vue d'une utilisation ou de la réalisation de projets ne relevant pas des missions pédagogiques ou des missions confiées aux utilisateurs. Chaque utilisateur se voit attribuer des codes d'accès en fonction de ses besoins (accès Internet, accès aux applications, accès à des serveurs particuliers, etc.). Les codes d'accès attribués sont strictement personnels et ne peuvent être prêtés. Chaque utilisateur est responsable de l'utilisation qui en est faite. Le nom d'utilisateur et le mot de passe sont imposés par le service informatique. Ils vous sont communiqués à votre entrée dans l'établissement. Chaque utilisateur s'engage à ne pas communiquer son nom d'utilisateur et son mot de passe à une tierce personne.
L'utilisateur préviendra le responsable informatique si un code d'accès ne lui permet plus de se connecter, s'il soupçonne que son compte a été usurpé. D'une façon plus générale, il informera, par l'intermédiaire de son enseignant ou formateur, le service informatique de toute anomalie qu'il pourrait constater.
Toutes les fiches formalisées utilisées pour communiquer avec le service informatique sont accessibles sur le serveur de fichiers en version électronique ou dans les salles des professeurs en version papier.

Seules les fiches officielles formalisées, dument remplies et signées par un enseignant ou un formateur feront l'objet d'une prise en charge par le service informatique. Toute autre action de communication avec le service informatique via un autre moyen ne peut être prise en compte, et la demande d'intervention sera ignorée.

III/ RESPECT DES REGLES DE LA DEONTOLOGIE INFORMATIQUE

Chaque utilisateur, qui est juridiquement responsable de l'usage qu'il fait des ressources informatiques, 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
- d'altérer, de modifier des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau ou à l'établissement, 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 ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau
- de modifier ou de détruire des informations sur un des systèmes
- de se connecter ou d'essayer de se connecter sur un site sans y être autorisé
- Sur des ressources externes, notamment les sites web, blogs ou réseaux sociaux, l'utilisateur veillera à ne pas communiquer des informations professionnelles non vérifiées ou pouvant nuire à l'ORT ou compromettre son image, ainsi que des informations à caractère confidentiel. Par ailleurs, il ne s'exprimera au nom de l'ORT qu'avec son autorisation.

La réalisation d'un programme informatique ayant de tels objectifs est également interdite.
Si dans l'accomplissement de son travail ou de ses missions, l'utilisateur est amené à constituer des fichiers, il est rappelé que la loi " informatique et libertés " impose, préalablement à leur constitution, que les fichiers comportant un traitement de données nominatives fassent l'objet d'une déclaration ou d'une demande d'avis auprès de la Commission Nationale Informatique et Libertés (CNIL).

IV/ UTILISATION DES LOGICIELS

L'utilisateur ne peut installer un logiciel qu'après avis du service informatique compétent. L'utilisateur ne devra en aucun cas :

- installer des logiciels à caractère ludique
- faire une copie d'un logiciel commercial
- contourner les restrictions d'utilisation d'un logiciel
- développer des programmes constituant ou s'apparentant à des virus, malware, spyware ou cheval de troie

V/ UTILISATION DES MOYENS INFORMATIQUES

Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. **Il informe immédiatement l'enseignant ou le formateur de toute anomalie constatée car il est la seule personne habilitée à transmettre le problème au service informatique**. 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. L'utilisation des ressources doit être rationnelle et loyale afin d'en éviter la saturation.
Tout ordinateur propre à une personne ou à une société, doit être connecté au réseau par l'intermédiaire d'un informaticien de l'établissement. Ce dernier s'assure en particulier que les règles de sécurité sont bien respectées.

Un utilisateur ne doit jamais quitter un poste de travail sans se déconnecter.

VI/ INFORMATION DES UTILISATEURS SUR LA GESTION DES SYSTEMES ET RESEAUX INFORMATIQUES

▪ Responsabilités de l'administrateur système / réseau

L'administrateur système / réseau est la personne qui gère les machines connectées au réseau de l'établissement ainsi que les serveurs sur lesquels sont installés les différents services mis à la disposition des utilisateurs (services Internet, applications, services pédagogiques, services pour la recherche et la documentation).
L'administrateur a la charge de la bonne qualité du service fourni aux utilisateurs dans la limite des moyens alloués. Il a le droit d'entreprendre toute démarche nécessaire au bon fonctionnement des moyens informatiques de l'établissement.
L'administrateur a 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 informatiques.
L'administrateur a le devoir d'informer immédiatement le responsable informatique de l'établissement (ou son suppléant) de toute tentative d'intrusion sur un système, ou de tout comportement délictueux d'un utilisateur.
L'administrateur doit impérativement respecter la confidentialité des fichiers des utilisateurs.

▪ Surveillance des utilisateurs

Il incombe à l'établissement et aux équipes pédagogiques de garder la maîtrise des activités liées à l'utilisation des services proposés, notamment en exerçant une surveillance ponctuelle des activités des utilisateurs via des outils de surveillance réseau, de manière à pouvoir intervenir rapidement en cas de problème, à repérer et faire cesser tout comportement pouvant devenir dangereux. L'ensemble des services utilisés génère, à l'occasion de leur emploi, "des fichiers de traces". Ces fichiers sont essentiels à l'administration des systèmes. Ils servent en effet à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers contiennent des informations.
Par exemple, chaque site Internet visité est lié à une date, une heure et au numéro de la machine émettrice. Toutes ces informations sont conservées durant une durée maximale d'un an par le service informatique. Ce type de traces existe pour l'ensemble des services Internet. Ces fichiers ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'une procédure judiciaire et après accord du Directeur ces fichiers peuvent être mis à la disposition ou transmis à la justice.

Cas particulier sur les flux chiffrés :

Parmi les flux qui transitent sur le réseau, les flux sécurisés constituent un cas particulier.
Le protocole **HTTPS** offre des possibilités d'authentification et de chiffrement pour les sites web nécessitant un certain niveau de sécurité dans leurs échanges avec les navigateurs web.
Pour ce faire, HTTPS fait usage du protocole SSL/TLS qui utilise des méthodes de cryptographie.
Ainsi, en principe, l'utilisation du protocole SSL/TLS permet d'assurer :

- L'authentification de l'une ou des deux parties communicantes
- La confidentialité des échanges
- L'intégrité des données échangées

Le flux étant chiffré entre le poste utilisateur et le serveur web, il n'y a pas de moyen de contrôle sur son contenu. Le filtrage des sites et l'antivirus sont, de ce fait, inopérants. Des sites mal intentionnés pourraient donc utiliser ce protocole pour introduire sur le réseau du contenu indésirable à l'insu de l'ORT.

Afin de protéger l'intégrité du réseau de l'établissement, un décryptage SSL/TLS est opéré.

Seuls les sites bancaires, de protections sociales, et les webmails (Gmail, Yahoo,…) ne sont pas concernés par ce dispositif afin de conserver le secret des correspondances.

- **Les virus**

Des outils sont également mis en place pour protéger les postes des utilisateurs contre les virus.
Les logiciels anti-virus sur les postes des utilisateurs sont paramétrés avec la stratégie suivante : Si un virus est détecté, le logiciel tente de réparer le fichier, si la tentative échoue, le fichier est détruit.
Un logiciel d'anti-virus est également mis en place sur le serveur Internet évitant ainsi de recevoir des virus et aussi d'en émettre à l'extérieur de l'ORT LYON.
D'autres logiciels pourront être mis en place pour protéger au mieux les données des utilisateurs et les applications de l'établissement.

- **L'accès Internet**

Chaque classe, section, formation ou service, ne bénéficient pas systématiquement de l'accès au réseau Internet. Cela dépend de la libre appréciation de l'usage de l'outil Internet par les responsables pédagogique, de formation, d'alternance et de service. En cas d'abus constaté sur le réseau Internet (par exemple: visite de sites illicites*, de sites sans rapport à la pédagogie ou de téléchargements abusifs) le service informatique informe au plus tôt le responsable concerné qui est libre de prendre la décision de couper Internet sans préavis à une classe, section, formation ou service selon son domaine de responsabilité.

*Les contenus illicites sont des propos ou la promotion d'activités interdits et punis par la loi française :

- La pédophilie et pédopornographie
- La diffamation, l'injure, l'apologie des crimes contre l'humanité
- La provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée
- Le proxénétisme, le racolage passif, l'intermédiation
- Le révisionnisme
- La promotion de l'anorexie
- L'atteinte à l'intimité et à la vie privée
- Les jeux d'argent non agréés par l'ARJEL (L'Autorité de Régulation des Jeux En Ligne)
- La contrefaçon de droit d'auteur, de marque, de dessins et modèles

Le service informatique se réserve le droit de bloquer certaines ressources Internet dans le but d'épargner les dérives illicites afin d'optimiser au maximum la rapidité du réseau Internet et enfin pour garantir les performances, la sécurité du réseau informatique interne de l'ORT LYON.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose au retrait de son compte informatique, ainsi qu'aux poursuites disciplinaires et pénales, prévues par les textes législatifs et réglementaires en vigueur.

Pour mémoire, les textes de référence en matière informatique sont :

- *la loi « informatique et libertés » de Janvier 1978 (création de la CNIL)*
- *la loi de Juillet 1978 sur l'accès aux documents administratifs*
- *la loi de 1985 sur la protection des logiciels*
- *la loi du 5 janvier 1988 relative à la fraude informatique*
- *la charte Renater (version révisée de 2005)*
- *LCEN : Décret relatif à la conservation des données d'identification*
- *La loi du 23 janvier 2006 dite « anti-terroriste »*
- *Décret n° 2011-219 du 25 février 2011 paru dans le Journal officiel du 1er mars*
- *LOPPSI 2 - Sécurité intérieure*
- *La loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieur*
- *Code du travail : article L. 121-8 / art. L1222-4 /art. L432-2 / art. L1121-1*

Date : ___ / ___ / _____

Nom et Prénom : _____ Signature : (précédée de la mention : *lu et approuvée*)