ÉCOLE CENTRALE LYON

FRENCH VERSION

CHARTE D'UTILISATION DES SYSTEMES D'INFORMATION DE L'ECL

L'Ecole Centrale de Lyon ci-après dénommée ECL

Préambule

Par "système d'information" s'entend l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition de l'«utilisateur».

L'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portable est également un des éléments constitutifs du système d'information.

Par «utilisateur», s'entend toute personne ayant accès, dans le cadre de l'exercice de son activité, aux ressources du système d'information quel que soit son statut.

Par «données professionnelles » s'entend l'ensemble des données, des fichiers, des traitements gérés par l'établissement au sein de son activité qu'elle soit de recherche, d'enseignement, administrative ou culturelle.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent et notamment, la sécurité, la performance des traitements et la conservation des données professionnelles.

La présente charte définit les règles d'usages et de sécurité que l'institution et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

L'ECL porte à la connaissance de l'utilisateur la présente charte.

Considérant les engagements de l'ECL :

Les ressources mises à disposition dans l'établissement sont prioritairement à usage d'enseignement, de recherche, culturel et professionnel. Toutefois l'ECL est tenue de respecter la vie privée de chacun.

Considérant les engagements de l'utilisateur :

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès.
Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique et de déontologie.

Les utilisateurs ont une responsabilité particulière dans l'utilisation qu'ils font des ressources mises à leur disposition par l'institution.
L'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.
Il est arrêté ce qui suit :

ARTICLE I. CHAMP D'APPLICATION

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'établissement ainsi qu'à l'ensemble des utilisateurs.

ARTICLE II. CONDITIONS D'UTILISATION DES SYSTEMES D'INFORMATION

Section II.1 Utilisation et vie privée

Dans le cadre de son activité, les *systèmes d'information* sont mis à la disposition de l'utilisateur.

L'utilisation à des fins privées doit être non lucrative et raisonnable quantitativement, tant dans la fréquence que dans la durée. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des systèmes d'information doit demeurer négligeable au regard du coût global d'exploitation.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet. Cet espace devra être dénommé « privé-personnel ». Le stockage et la sauvegarde des données à caractère privé incomberont à l'utilisateur.

Section II.2 Continuité de service : gestion des absences et des départs

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies avec le responsable ou les responsables désignés au sein de l'institution ou des structures dont dépend l'utilisateur.

ARTICLE III. PRINCIPES DE SECURITE

Section III.1 Règles de sécurité applicables

L'institution, son ministère de tutelle, ses fournisseurs d'accès et ses partenaires techniques extérieurs mettent en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les mots de passe (ou tout autre système d'authentification) constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des systèmes d'information mis à sa disposition lui impose de respecter les consignes de sécurité, les règles relatives à la gestion des mots de passe; notamment :

- de choisir un mot de passe sûr, n'ayant aucun lien avec l'environnement familier de l'«utilisateur» ;
- de changer de mot de passe régulièrement, si les applications le permettent ;
- de ne pas écrire son mot de passe sur un support facilement accessible ;
- de garder strictement confidentiel son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers; En cas de doute sur cette confidentialité, il incombe à l'utilisateur de changer immédiatement ses mots de passe ;
- de respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre utilisateur, ni chercher à les connaître.
- L'utilisateur est responsable des opérations effectuées grâce à son identifiant et son mot de passe; il ne peut en aucun cas les divulguer ou s'approprier ceux d'un autre utilisateur.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

- de la part de l'institution :
    - veiller à ce que les ressources sensibles ne soient pas accessibles en cas d'absence (en dehors des mesures de continuité mises en place par la hiérarchie) ;
    - limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

- de la part de l'utilisateur :
    - Si l'utilisateur ne bénéficie pas d'une habilitation explicite, il doit s'interdire d'accéder ou tenter d'accéder à des ressources du système d'information, même si cet accès est techniquement possible ;
    - ne pas connecter directement aux réseaux des matériels non confiés ou non autorisés par l'établissement ;
    - ne pas installer, télécharger ou utiliser sur le matériel de l'établissement, de logiciels ou progiciels sans autorisation explicite ;
    - se conformer aux dispositifs mis en place par l'établissement pour lutter contre les virus et les différentes attaques pouvant nuire aux systèmes d'information.

Section III.2 Devoirs de signalement et d'information
L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, etc. : il signale également à la personne responsable du site toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation.

Section III.3 Mesures de contrôle de la sécurité
L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'établissement se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- qu'une maintenance à distance est précédée d'une information de l'utilisateur ;
- que toute information bloquante ou présentant une difficulté technique d'acheminement à son destinataire, peut être isolée, le cas échéant supprimée (information de type virus, logiciel espion, pourriel ou spam).

L'établissement informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Les personnels en charge des opérations de contrôle sont soumis au secret professionnel. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction en particulier lorsque ces informations sont couvertes par les secrets des correspondances ou relèvent de la vie privée de l'utilisateur dés lors que ces informations ne remettent pas en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du service. Par ailleurs, les personnels en charge des opérations de contrôle sont également soumis à la loi et ne peuvent pas diffuser d'information à leur hiérarchie sauf cas de plainte auprès du procureur de la république.

ARTICLE IV. COMMUNICATIONS ELECTRONIQUES

Section IV.1 Messagerie électronique
L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de l'établissement.

(a) Adresses électroniques

L'établissement s'engage à mettre à la disposition de l'utilisateur une boîte à lettres nominative lui permettant d'émettre et de recevoir des messages électroniques.

L'adresse électronique nominative est attribuée à un utilisateur. Par norme sous la forme prenom.nom@ec-lyon.fr sauf cas d'homonymie.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place si elle est exploitée par un service ou un groupe d'utilisateurs.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une structure institutionnelle ou un groupe d'«utilisateurs», relève de la responsabilité exclusive de l'ECL : ces adresses ne peuvent être utilisées sans autorisation explicite.

(b) Contenu des messages électroniques

Les messages électroniques permettent d'échanger principalement des informations à vocation liées à l'activité directe de l'ECL. En toutes circonstances, l'utilisateur doit adopter un comportement responsable et respectueux des dispositions contenues dans la présente charte.

Tout message sera réputé lié a l'institution sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un espace privé de données. Le sujet de la correspondance électronique devra commencer par la mention «privé-personnel».

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui.

(c) Émission et réception des messages

L'utilisateur doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.
Il est interdit de diffuser des messages à un groupe de personnes dès lors qu'il existe une liste de diffusion institutionnelle dédiée pour cet usage.

(d) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles[6] 13691 et 136911 du code civil.
L'utilisateur doit en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

(e) Stockage et archivage des messages

Chaque utilisateur doit organiser et mettre en oeuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.
À ce titre, il doit notamment se conformer aux règles définies dans la présente charte.

Section IV.2 Internet
Il est rappelé que le réseau Internet est soumis à l'ensemble des règles de droit en vigueur.

L'utilisation de la technologie Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'ECL

L'ECL met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

Internet est un outil de travail ouvert à des usages professionnels (administratifs, pédagogiques, recherches ou culturels) : il peut constituer le support d'une communication privée telle que définie en section II.1 dans le respect de la législation en vigueur. En complément de ces dispositions légales et au regard de la mission éducative de l'établissement, la consultation volontaire de contenus illicites depuis les locaux de l'établissement, est proscrite.

L'établissement se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

L'établissement, son ministère de tutelle, ses fournisseurs d'accès ou ses partenaires techniques extérieurs se réservent le droit d'interdire certains accès, protocoles de communication, programmes ou modules pouvant porter atteinte à la sécurité.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'établissement

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formations ou de campagnes de sensibilisation.

Section IV.3 Téléchargements
Tout téléchargement de fichiers, notamment de sons ou d'images, sur le réseau Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle.

L'établissement se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'établissement, code malicieux, programmes espions …).

ARTICLE V. TRAÇABILITE

L'établissement est dans l'obligation légale de mettre en place un système de journalisation, archivage des accès Internet, de la messagerie et des communications numériques échangées. Il est tenu de recueillir et conserver des informations sur les utilisateurs et peut, dans le cadre d'une enquête judiciaire, être dans l'obligation de les fournir aux autorités compétentes.

Préalablement à cette mise en place, l'institution procédera, auprès de la commission nationale de l'informatique et des libertés, à une déclaration, qui mentionnera notamment la durée de conservation des traces et durées de connexions, en application de la loi n° 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004801 du 8 août 2004 et n°2011219 du 25 Février 2011.
L'utilisateur peut demander à l'Ecole la communication des informations nominatives le concernant et les faire rectifier en application des dispositions de la loi.

ARTICLE VI. RESPECT DE LA PROPRIETE INTELLECTUELLE

L'établissement rappelle que l'utilisation des moyens informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

ARTICLE VII. RESPECT DE LA LOI INFORMATIQUE ET LIBERTES

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 7817 du 6 janvier 1978 dite «Informatique et Libertés» modifiée par la loi n° 2004801 du 6 août 2004.

Les données à caractère personnel sont des informations qui permettent sous quelque forme que ce soit directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi «Informatique et Libertés».

En conséquence, tout utilisateur souhaitant procéder à un tel traitement devra en informer préalablement le Correspondant Informatique et Libertés (CIL) désigné par l'Établissement à la Commission Nationale Informatique et Libertés.

Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'Information.

Ce droit s'exerce auprès du Correspondant Informatique et Libertés.

ARTICLE VIII. LIMITATIONS DES USAGES

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation, le directeur ou les responsables sécurité du système d'information pourront, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles, est passible de sanctions.
Elles sont décidées par la section disciplinaire de L'ECL prévue à l'article L 712-4 du code de l'éducation. Les sanctions encourues sont fixées par le décret n° 92-657 du 13 juillet 1992 modifié fixant la procédure disciplinaire dans les Etablissements Publics à caractère Scientifique, Culturel et Professionnel (EPSCP).

ARTICLE IX. ENTREE EN VIGUEUR DE LA CHARTE

La présente charte est adossée au règlement intérieur et en constitue un élément indissociable. Son approbation se fait dans les mêmes conditions de forme que le règlement intérieur de l'établissement.

Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des systèmes d'Information.

ENGLISH VERSION

ECL IT SYSTEM CHARTER

Hereinafter, the Ecole Centrale de Lyon is referred to as ECL

Preamble

"IT" refers to all hardware, software, applications, data-bases and telecoms networks available to the "user".

Nomad equipment such as personal assistants, laptops and cell-phones are also included under "IT system".

"User" refers to all those, of whatever status, having access to the IT system resources by virtue of their occupation.

"Professional data" refers to all data, files and processing managed by ECL, whether for research, teaching, administrative or cultural purposes.

The performance of the IT system presupposes that all legal and regulatory requirements are respected, notably as concerns security, processing and storage of professional data.

This Charter lays down the rules of use and security that the institution and the user undertake to respect, and specifies respective rights and obligations.

ECL brings the Charter to the attention of the user.

Regarding ECL's undertakings:

The IT resources available in the School are primarily intended for teaching, research, cultural and professional purposes. Nevertheless, ECL undertakes to respect users' privacy.

Regarding the user's undertakings:

Users are responsible for the use they make of the IT system available to them in whatever place.
Users shall respect the confidentiality of information and documents to which they have access. This includes respecting ethical and deontological rules.

Users have a particular responsibility for the use they make of the resources made available to them by the School.

Users shall respect the obligations entailed by their status or contract.

It is provided as follows:

ARTICLE I. FIELD OF APPLICATION

The rules for use and security contained in the present Charter apply to the School and to all users.

ARTICLE II. CONDITIONS OF USE OF IT SYSTEMS

Section II.1 Use of IT and privacy

IT systems are made available to users in the context of their work.

Any private use must be non-profit-making and quantitatively reasonable in frequency and duration. It should not interfere with the user's work and the time devoted to it or with the functioning of the institution.

At all events, extra costs related to private use of the IT systems must remain negligible in comparison with overall costs.

All information is deemed to be work-related except for data explicitly designated by the user as being private. It is thus up to users to store their private data in a dedicated data space, which should be labelled "Private-personal". Storage and back-up of private information is the responsibility of the user.

Section II.2 Continuity of service: management of absences and departures

Users are in charge of their private data spaces. On finally leaving the department or the School, they shall destroy their private data spaces, and the administration shall not be responsible for conserving such spaces. Rules for conserving work-related data are determined with the person or persons in charge of the institution or structures to which the user belongs.

ARTICLE III. PRINCIPLES OF SECURITY

Section III.1 Applicable security rules

The School, the Ministry of Education, the School's access providers and external technical partners implement the appropriate mechanisms to protect the IT systems made available to the users.

Users are hereby informed that passwords (and any other verification system) are a security measure to prevent malevolent or abusive behaviour. These measures should not be understood as conferring a personal status on the IT tools they protect.

The levels of access available to a given user are determined according to that user's mission. The security of the IT systems available to him or her requires that the security instructions and password rules be adhered to, and in particular:

- Choosing a safe password, unrelated to the user's everyday environment;
- Changing passwords regularly if applications permit;
- Never writing passwords down where they would be easily accessible;
- Keeping passwords strictly confidential and never disclosing them to any third party; if there is any doubt as to secrecy, the user should immediately change the password;
- Respecting access rules and in particular never using the username or password of another user or trying to discover them;
- Users are responsible for operations performed via their user name and password, and must never divulge them or use another user's.

The security of the resources made available to the user entails certain precautions:

- On the part of the School:
    - Making sure that sensitive resources are not accessible in case of absence (apart from the officially sanctioned means of ensuring continuity of service);
    - Restricting access to only those resources to which the user is specifically entitled.

- On the part of the user:

    - Users must not attempt to access IT resources to which they are not specifically entitled, even if to do so is technically feasible;
    - Equipment that has not been entrusted to the user or is not authorized by the School must not be connected up directly to the IT networks;
    - Software is not to be installed, downloaded or used on School equipment without explicit authorisation;
    - Users must respect the measures set out to combat viruses and other attacks that could harm the IT systems.

Section III.2 Obligation to inform

Users are to report to their superiors any malfunction or abnormality they may discover: intrusion into the IT system, etc.; they are also to report to the site manager any possibility of unentitled access to resources.

Section III.3 Security control measures

Users are informed that:

- The School may undertake any corrective or curative maintenance or assessment operations (remote or otherwise) on the resources at their disposal;
- Users receive warning of remote maintenance;
- Any data causing blockage or a technical difficulty in transmission may be quarantined or deleted: e.g., virus, spyware, spam, etc..

Users are informed that the IT system may be put under surveillance and control for purposes of statistics, traceability, optimisation or detection of misuse.

Personnel in charge of control operations are bound to confidentiality and may not divulge information they become aware of in their work, notably when the information is part of correspondence or the user's private domain, so long as such information does not threaten the technical functioning or security of applications or the interest of the School. Personnel in charge of control operations are also subject to the law, and may not divulge information to their superiors except in case of action by the state prosecution department.

ARTICLE IV. ELECTRONIC COMMUNICATION

Section IV.1 E-mail

E-mail is an essential element in optimizing work and sharing information within the School.

(a) E-mail addresses

The School undertakes to make a nominative mail box available to the user to send and receive e-mail.

Each user is attributed a specific e-mail address, in the form <firstname.surname@ec-lyon.fr> except in case of homonyms.

A function or organisation based e-mail address can be created for departments or groups of users.

The management of e-mail addresses in School mailing lists and referring to School structures or user groups is the exclusive responsibility of ECL: such addresses may not be used without explicit authorisation.

(b) E-mail message content

E-mail is principally intended for the exchange of messages directly concerning ECL activity. Users must at all times behave responsibly and respectfully towards the provisions of the present Charter.

All messages are to be deemed School-related unless they are specifically and explicitly designated private or are stored in a private data space: the subject-line of such messages should begin "Private-personal" ("*privé-personnel*").

To protect efficient service, restrictions may be enforced.

Messages with illegal content of any sort, particularly when contrary to the law on freedom of expression or infringing privacy, are forbidden.

(c) Sending and receiving messages

Users are responsible for ensuring that e-mail is sent only to intended recipients, so as to avoid mass mailing, unnecessarily overloading the network and impairing service.
E-mail shall not be sent to groups of persons when a corresponding institutional mailing list exists.

(d) Legal status and value of e-mail

E-mail exchanged with third parties may, legally, constitute a contractual relationship under the provisions of articles 13691 and 136911 of the French *Code Civil*.
Users should therefore be attentive to the nature of e-mail exchanged, as is also the case for land mail.

(e) Storing and archiving e-mail

Users should arrange and implement means of storing e-mail that may be necessary or simply useful as evidence.
In this regard, they are to respect the rules stipulated in the present Charter.

Section IV.2 Internet

Users are reminded that the Internet is subject to all the legal provisions in force.

Internet (and, by extension, intranet) technology is an essential element in optimising work and making available and sharing information inside and outside of ECL.

ECL makes Internet access available to the user whenever possible.

The Internet is a work tool available for professional (administrative, teaching, research and cultural) use: it may also be a means of private communication, as defined in section II.1 in line with current legislation. In addition to such legal provisions, the educational mission of the School means that intentional consultation of illegal content on School premises is forbidden.

The School reserves the right to filter or ban access to certain websites and to monitor or check which websites have been visited and for what duration.

The School, the Ministry, the School's access providers and outside technical partners reserve the right to ban access to certain sites, communication protocols, programs or applications liable to infringe security.

Internet access is allowed only via the security applications implemented by the School.

Users are informed, by training sessions and awareness campaigns, of the risks and limits inherent to the use of the Internet.

Section IV.3 Downloading

Downloading of files, and especially audio or video files, from the Internet must respect intellectual property rights.

The School reserves the right to restrict downloading of heavy data files or files incurring a security risk for the IT systems: viruses liable to impair system functioning, malware, spyware, etc.

ARTICLE V. TRACEABILITY

The School is under a legal obligation to implement a journal archiving Internet access and exchange of e-mail and digital communication. It is obliged to collect and store information regarding users and may, in case of legal inquiries, be obliged to provide such information to the relevant authorities.

Before implementing the above, the School will submit a declaration to the French data protection commission (*Commission Nationale de l'Informatique et des Libertés*: CNIL*)*, specifying in particular the period of conservation of traces and durations of connection, in line with Law n° 7817 dated 6 January 1978, concerning IT, data files and liberties, as updated by Laws n°2004801 dated 8 August 2004 and n° 2011219 dated 25 February 2011.
Users may ask the School for and may correct information specifically concerning them, in line with the provisions of the Law.

ARTICLE VI. RESPECT OF INTELLECTUAL PROPERTY

The School draws the attention of users to the fact that using its IT resources presupposes respecting its rights of intellectual property and those of it s partners and, more generally, of all third parties.

In consequence, users shall:

- Use software according to the license conditions;
- Not reproduce, copy, share or alter the software, data-bases, Web pages, texts, images, photographs or other creations protected by copyright or private rights without prior authorization from the right-holders.

ARTICLE VII. RESPECT OF THE *INFORMATIQUE ET LIBERTÉS* DATA PROTECTION LAW

Users are to respect the legal provisions concerning automated processing of personal data, in line with the "*Informatique et Libertés*" (IT and liberty) law n° 7817 dated 6 January 1978 and updated by law n° 2004801 dated 6 August 2004.

"Personal data" refers to information which may in any way, directly or indirectly, enable identification of the persons to which it relates.

Creation of any kind of data file including this type of information, even when produced by crossing or linking pre-existing files, is subject to the preconditions laid out in the *Informatique et Libertés* law.

Users wishing to undertake such data processing must therefore inform in advance the *Informatique et Libertés* agent appointed to the national *Informatique et Libertés* commission by the School.

Under the provisions of the same law, users have a right of access to and correction of all data related to them, including data on their IT system use.

This right is implemented via the *Informatique et Libertés* officer.

ARTICLE VIII. RESTRICTION OF USE

In case of failure to respect the rules laid down in the present Charter or the instructions contained in the user guides, the Director or IT security officers may restrict access as a precaution without prejudice to any legal action or penalties.

Any misuse of the resources made available to the user for non-work-related purposes may be penalised.
Penalties will be determined by the disciplinary body of ECL in accordance with Article L 712-4 of the Education Code, and set by the modified Decree n° 92-657 of 13 July 1992, laying down disciplinary procedures in public scientific, cultural and occupational establishments (EPSCPs).

ARTICLE IX. EFFECTIVE APPLICATION OF THE CHARTER

The present Charter is appended to the School Rules, of which it is an integral part. It is accepted under the same conditions as the Rules.

The present text overrides and replaces all previous documents or charters relating to IT use.