CHARTER RELATING TO THE USE OF THE INFORMATION SYSTEMS OF THE ECOLE CENTRALE DE LYON V.2018 APPROVED BY THE BOARD of MANAGEMENT SESSION OF 18/10/2018

It is hereby understood that the present charter is annexed to the internal rules and that it cannot be separated from them.
The Ecole Centrale de Lyon shall be referred to in the following as ECL.

Preamble

The term “Information system” shall cover all the hardware, software, applications, databases and telecommunications networks liable to made available to the “user”.

Nomad computer devices such as personal assistants, laptop computers and cell phones are also items which constitute the information system.

The term “user” shall cover any physical person having access, in the framework of carrying out their activity, to the information system resources, whatever their status.

The term “professional data” shall cover all the data, files and processes managed by the establishment in its activity whether it be research or teaching, or of an administrative or cultural nature.

The efficient operation of the information system depends on compliance with the legislative and regulatory provisions in force, in particular regarding the security, the performance of processes, and the conservation of professional data.
(*) Non-exhaustive reminder of the main laws on the last page.
The present charter defines the rules of utilisation and security that the institution and the user undertake to comply with: it stipulates the rights and obligations of each person.

The ECL hereby makes known the present charter to the user.

Regarding the obligations of the ECL:

The resources made available in the establishment are above all intended for teaching, research, cultural and professional purposes. However, the ECL is bound to respect the private life of each person.

Regarding the user’s obligations:

The user is responsible, in all places, for the use they make of the information system to they have access.
They are bound to keep confidential the information and documents to which they have access. This obligation implies compliance with the rules of ethics and deontology.

The users have a specific responsibility regarding their utilisation of the resources made available to them by the institution.
The user is bound to abide by the obligations resulting from their status or their contract.
Consequently, the following has been decided:

ARTICLE I. SCOPE OF APPLICATION

The rules of utilisation and security featuring in the present charter are applicable to the establishment and to all the users.

ARTICLE II. CONDITIONS OF UTILISATION OF INFORMATION SYSTEMS

Section II.1 Utilisation and private life

The information systems are made available to the user in the framework of their activity.

The utilisation of said systems for private uses must be for non-profit purposes and be of a reasonable quantity regarding both frequency and duration. It must not harm the quality of the user's work, the time they devote to it or the efficient operation of the service.

Whatever the case, the additional cost resulting from the residual private use of the information systems must remain negligible in relation to the global operating cost.

All information is reputed professional to the exclusion of data designated by the user as belonging to their private life. Thus, the user is responsible for storing their private data in a space explicitly intended for this purpose. This space shall be named "private-personal". The storage and saving of private data is the responsibility of the user.

Section II.2 Service continuity: management of absences and departures

The user is responsible for the space in which they keep their private data. When they finally leave the service or the establishment, they shall destroy the space they allot to their private data, as the administration cannot be held liable for the conservation of this space. The measures taken to conserve professional data shall be defined with the managers appointed in the institution or the structures on which the user depends.

ARTICLE III. PRINCIPLES OF SECURITY

Section III.1 Applicable security rules

The institution, the ministry to which it answers, its access providers and its external technical partners implement appropriate protective mechanisms for the information systems made available to the users.

The user is hereby informed that the passwords, means of access (or any other system of authentication) are means used to ensure security and to avoid any improper or abusive utilisation. These means do not bestow any personal nature to the computer tools thus protected.

The levels of access open to the user are defined as a function of the mission entrusted to them. The security of the information systems made available to them requires compliance with security instructions and the rules relating to password management; in particular the user must:

- choose a safe password, without any link to the environment familiar to the “user”;
- choose passwords of sufficient complexity and not reuse the same passwords on different systems;
- regularly change the password, if the applications so permit;
- not write their password on an easily accessible medium;
- keep their password(s) strictly confidential and not disclose them to a third person. In case of doubt regarding this confidentiality, it is the user’s responsibility to immediately change their passwords and inform the Information Systems Department;
- comply with access management, in particular the user shall not use the passwords of other users or seek to know them;
- take responsibility for the operations performed by virtue of their login and password.

Furthermore, the security of the resources made available to the user requires several precautions:

- from the institution:
    - to ensure that sensitive resources are not accessible in the case of absence (excluding the measures of continuity organised by the management);
    - to limit access to only the resources for which the user is expressly authorised.

- from the user:
    - In a professional framework, the users must use the digital services made available by the École Centrale de Lyon, its laboratories and co-contracting partners (email, file sharing, collaborative working platform, etc.) and not the tools supplied by an external provider (whether free or otherwise) which may expose sensitive information to external parties in an uncontrolled manner.
    - If the user has not been given explicit authorisation, they must abstain from accessing or attempting to access the resources of the information system, even if this access is technically possible;
    - Not to directly connect with networks hardware that has not been entrusted to them or authorised by the establishment; and in addition they shall not activate Wi-Fi points or interact with the establishment’s radio frequency.
    - The user shall not install, download or use software or software packages on the establishment’s hardware without explicit authorisation;
    - The user must follow the instructions of the ISD to ensure in particular that the configuration of their hardware complies with good security practices (application of security patches, encryption, antivirus, etc.)

Section III.2 Obligation to alert and inform

The user must inform their management within the shortest time possible of any malfunctioning, loss, theft or other anomaly discovered such as intrusion in the information system, etc.: they must also inform the person responsible on the site of any possibility of access to a resource that does not correspond to their authorisation.

Section III.3 Control and security measures

The user is hereby informed:

- that to perform corrective or ongoing maintenance, the establishment reserves the right to carry out interventions (possibly remotely) on the resources made available to them;
- that the user is informed beforehand of remote maintenance;
- that any information generating a block or which is technically difficult to route to its addressee may be isolated and destroyed if necessary (viruses, spyware, spam).
- that the information system can give rise to monitoring and control for statistical, traceability, optimisation, security and abuse detection purposes.

Section III.4 Obligations of the administrators of the information systems

The personnel responsible for administrating the information systems are subject to professional secrecy. They cannot therefore disclose information that they may learn in the framework of their office, in particular when said information is protected by the secrecy of correspondence or pertains to the private life of the user, provided that this information does not jeopardise the efficient technical operation of the applications, their security, or the interests of the department. Furthermore, the persons responsible for the information systems are also subject to the law and cannot disclose information to their management except in the case of a judicial complaint made to the public prosecutor.

ARTICLE IV. ELECTRONIC COMMUNICATIONS

Section IV.1 Electronic messaging

The utilisation of the messaging service is one of the essential elements for optimising work and sharing information in the establishment.

(a) Email addresses

The establishment undertakes to make available to the user a personal mailbox allowing them to send and receive emails.

The personal email address is assigned to one user. The standard used takes the format of first name.family name@(XXX.)ec-lyon.fr except in the case of homonyms.

A functional or organisation email address can be generated if it is used by a service or a group of users.

The management of email addresses corresponding to lists of institutional distribution, designating an institutional structure or a group of users, remains the exclusive responsibility of the ECL: these addresses cannot be used without explicit authorisation.

(b) Content of electronic messages

Emails allow exchanging information primarily and directly linked to the ECL's activity. Whatever the circumstances, the user shall adopt responsible behaviour in compliance with the provisions contained in the present charter.

Every message shall be considered linked to the institution unless it includes a specific and explicit mention indicating its private nature or if it is stored in a private storage space. The subject of the email shall start with the mention "private-personal".

Limitations may be implemented to maintain the efficient operation of the services.

Messages including content of an illegal nature of any kind are prohibited. This applies in particular to content contrary to the provisions of the law on the freedom of expression or detrimental to the private life of other persons.

(c) Transmission and reception of messages

The user must ensure that the messages they send are sent only to the addressees concerned in order to avoid the mass diffusion of messages that congest the messaging service unnecessarily and deteriorate the service.
It is forbidden to diffuse messages to a group of persons when an institutional distribution list exists for this purpose.

(d) Status and legal value of messages

Emails exchanged with third parties may constitute a legal contract, under reserve of compliance with the conditions stipulated in articles[6] 13691 and 136911 of the civil code.
Therefore, the user must exercise vigilance regarding the nature of the emails they exchange in the same way as for traditional letters.

(e) Storage and archival of emails

Each user must organise and employ the resources necessary to conserve emails that may be vital or simply useful as elements of proof.
Consequently, they must conform to the rules set out in the present charter.

Section IV.2 Internet

It is hereby recalled that the Internet network is subject to all the legal rules in force.

The use of Internet technology (and by extension intranet) is one of the essential elements underlying the optimisation of work, and sharing and accessing information inside and outside the ECL.

The ECL makes Internet access available to the user whenever possible. The ECL network is intended to transmit information produced by the ECL's activities: teaching, research, technical development, technological transfer, the dissemination of scientific, technical and cultural information, experiments and new services of a technically innovative nature.
Therefore, any access by unauthorised third parties for commercial or non-commercial uses, whether remunerated or not, or for personal amusement, is forbidden.

Internet is a work tool open to professional uses (administrative, pedagogical, research and cultural): it can be considered as a medium for private communication as stipulated in section II.1 in conformity with the legislation in force. In addition to these legal provisions and with respect to the establishment's educational mission, the deliberate consultation of illicit content in the establishment's premises is forbidden.

The establishment reserves the right to filter or forbid access to certain sites, and to control before or afterwards the sites visited and the corresponding durations of access.

The establishment, its supervisory ministry, its access providers and its external technical partners reserve the right to prohibit certain accesses, communication protocols, and programs and modules liable to harm security.

This access is authorised only via the security systems implemented by the establishment.

The user shall be informed of the risks and limits inherent in using the Internet by way of training activities and awareness campaigns.

Section IV.3 Downloading

All downloads of files, especially of sounds and images, from the Internet must be done in compliance with intellectual property rights.

The establishment reserves the right to limit the downloading of certain large files or those that present a risk for the security of the information systems (virus liable to damage the efficient operation of the establishment's information system, malware, spyware, etc.).

ARTICLE V. TRACEABILITY

The establishment is legally obliged to set up a logging system that archives accesses to the Internet, messaging and the digital communications exchanged. Its purpose is to collect and conserve information on the users and, in the framework of a judicial investigation, the establishment may be obliged to supply said archives to the competent authorities.

ARTICLE VI. CONFORMITY WITH INTELLECTUAL PROPERTY RIGHTS

The establishment hereby recalls that the use of computer resources implies conformity with its intellectual property rights and those of its partners and more generally of all third parties holding such rights.

Therefore, each user must:

- use the software applications in conformity with their licences;
- not reproduce, copy, distribute, modify or use software applications, databases, web pages, texts, images, photographs or other creations protected by copyright or a private right, without having prior authorisation from the owners of these rights.

ARTICLE VII. CONFORMITY WITH THE LAW ON DATA PROCESSING AND CIVIL LIBERTIES AND THE GENERAL REGULATIONS ON DATA PROTECTION

The user is informed that the ECL is bound to conform to all the legal provisions applicable to the automatic processing of personal data, the most important of which are laws nos. 7817 of 6 January 1978 and 2018-493 of 20 June 2018 known as the "Law on Data Processing and Civil Liberties" and the General Data Protection Regulation (EU) 2016/679 of 27 April 2016.

Data of a personal nature are data in any form that permit the direct or indirect identification of the physical persons to whom they pertain.

These data are placed under the responsibility of the ECL, acting in its capacity of processing manager, in conformity with the principle of accountability (article 24 of the General Data Protection Regulation).

Each user has the right to consult, correct and oppose the data concerning them, including the data relating to the use of information systems.

This right is exercised by contacting the Delegate for Data Protection. (dpd.rgpd@listes.ec-lyon.fr)

ARTICLE VIII. LIMITATION OF UTILISATION

In the case of non-conformity with the rules stipulated by the present charter and the procedures defined in the user guides, the director or the information system security managers may, without prejudice to law suits or sanction procedures liable to taken out against personnel, limit the use of the resources as a provisional measure.

Any improper use of the resources made available to the user for extra-professional purposes is liable to sanctions.
The latter shall be decided by the disciplinary committee of the ECL as set out in article L 712-4 of the education code. The penalties incurred are stipulated by article R-811 of the education code.

ARTICLE IX. ENTRY INTO FORCE OF THE CHARTER

The present charter is annexed to the internal rules and is inseparable from them. Its approbation is subject to the same conditions of form as the establishment's internal rules.

The present document cancels and replaces all the other documents or charters relating to the utilisation of information systems.

LEGAL REMINDERS
This non-exhaustive list is provided for the purposes of information.

The school and the user are bound to conform to the following legal and regulatory provisions:

- Circular PM No.5725, signed on 17 July 2014, relating to the application of the Government Information Systems Security Policy;
- Decree no.2011-1425 of 2 November 2011 relating to the application of article 413-7 of the penal code relating to the protection of the nation's scientific and technological potential;
- Ruling of 3 July 2012 relating to the protection of the nation's scientific and technological potential.
- Inter-ministerial circular relating to the application of the procedure for protecting the nation's scientific and technological potential of 7 November 2012.

The use of computer resources in the school remains subject to the law.

- respect for people (no harm to private life or to the secrecy of correspondence, or insults or slander) and respect for information systems (crimes and offences against property); *Article 9 of the Civil Code, Articles: 226-1,226-15, 222-17, R 621-2, 226-10 of the Penal Code, art.432-9 amended by law no.2004-669 of 9 July 2004, Article 29 of the Law of 29 July 1881, Article 26, 27,34, 36 of Law no. 78-17 of 6 January 1978, art. 313-1 and following 323-1 to 323-7 amended by law no.2004-575 of 21 June 2004 of the Penal Code.*
- the protection of minors against degrading and violent content, or content favouring their corruption; *Article 227-24, 227-23 of the Penal Code, Law 2004-575 of 21 June 2004.*
- Conformity with public order in condemnation of racism, antisemitism and apology for crime; *Article 24 and 24a of the Law of 29 July 1881, Article L 323-1 and following of the Penal Code.*
- Non-infringement of copyright on on-lined literary, musical, photographic and audiovisual works, non-infringement of intellectual property relating to software. *Articles L 335-3, L 111-1, L 121-1, L 122-1, L 123-2, L 131-2 of the Intellectual property code*
- Protection against computer crime: unauthorised penetration into an automated system, destruction or modification of data, fraudulent introduction of data, interference with operation; *law of 5 January 1988 known as the "Jacques Godfrain law" and its 7 articles (323-1 à 323-7).*
- The law on the storage of connection data:
  "electronic communications operators shall conserve for the needs of investigation, evidence and the pursuit of penal violations: information permitting the identification of the user, data relating to the computer and communication terminals used, the technical characteristics and the date, time and duration of each communication, the data relating to additional services demanded or used and their providers, and the data permitting the identification of the addressee(s) of the communication."
  Decree no.2006-358 of 24 March 2006 Art. R. 10-13.- I