ÉCOLE NORMALE SUPÉRIEURE DE LYON

15 parvis René-Descartes
BP 7000, 69342 Lyon cedex 07
Tél. +33 (0)4 37 37 60 00
www.ens-lyon.fr

Information Systems Charter ENS de Lyon 2016

This Charter defines the General Conditions of Use of the Internet, networks and computing resources within the establishment, specifying the legal frame and the application of the law to help users be aware of their responsibilities.

Preamble

"Information Systems" means all the hardware and software resources that can be made available to the user. For reasons of network security, this also includes the personal equipment of users connected to the network of ENS de Lyon.

"User" means any person having access to computing resources regardless of their status.

Any use that is not defined by the Charter is only tolerated if it remains restricted. Any use for commercial, political or recreational means is prohibited.

Compliance with the law

The internet, networks and digital communication services are not lawless areas. Threats to the core values of education, including in particular the principles of religious, political and commercial neutrality, are also (but not exclusively) banned and if necessary sanctioned by criminal means:

- Infringement of the privacy of others;
- Defamation and insult;
- The provocation of minors to commit illegal or dangerous acts, fostering the corruption of a minor, exploitation of pornographic images of a minor, the dissemination of messages in a violent or pornographic way;
- Provocation to commit a crime and or commit suicide, provocation leading to discrimination, including racial hatred, or violence;
- The reproduction, representation or broadcasting of intellectual work
- Copies of commercial software for any purpose whatsoever, with the exception of a backup copy in the conditions provided for by the code of intellectual property.

Access to computing resources:

The user must respect the terms of connection (wired or wireless) devices to networks as specified by the Information Technology Department (ITD) or local computer technician.

The right of access to computing resources is strictly personal and non-transferable. Users are responsible for the use of computing resources accessed from their personal connection. If the user suspects that his/her password could be compromised, it should immediately be changed.

The IS Department or the local computer technician will not ask for the disclosure a user password.

The right of access is temporary. It is removed in the following cases:

- The function or status no longer justifies it.
- Failure to comply with the Charter.

Access to computing resources is provided to the user for business purposes and for purposes related to pedagogy, research or professional integration. Any stored data is presumed to be professional, unless its file name contains the words "private-personal".

E-mail

E-mail is primarily to exchange information related to the direct activity of the establishment. Any message will be deemed as being related to the institution unless it has a special and explicit reference indicating its private character. The subject of the e-mail correspondence should in this case start with the wording "private-personal".

In legal terms, e-mail messages exchanged with third parties can form a contract, subject to compliance with the conditions laid down by Articles 613691 and 136911 of the civil code. Users must therefore, be vigilant about the nature of the e-mail messages they exchange, as well as for paper mail.

Access to e-mail is granted according to the technical guidance of the IS Department. Giving a password to a third-party to pick up the user's mail is prohibited.

Before the deletion of their account, e-mail account holders will be informed by e-mail. They must then destroy or retrieve their private data.

Wireless networks

Only the IS Department may operate the Hertzian space of ENS de Lyon: apart from this strict framework, it is forbidden to put into operation a wireless access point. Particular attention must be paid to access points that are sometimes enabled by default on the following materials: hotspot, some printers, some network disks.

Commitments of the user:

- Users are responsible for their use of computer resources; They must commit to not perform any operations that can affect the operation of the network and the integrity of computer resources.

- If they detect a malfunction or security problem, users should immediately alert the IT department or their local computer technician to resolve the problem and if necessary to stop an attack in progress.

- When absent from their workstation, users must lock the session. If they have a laptop, it should be locked.

- The user agrees not to install software without ensuring that it is safe.

- Users are regularly victims of a phishing and should be particularly vigilant in reading their e-mail. A tool is also available in the e-service portal to check that an account has not been hacked.

- The IT Department can provide a tool to backup workstations. It is up to users to check that this tool works well on their desktop.

- Some software and operating systems offer security updates. Users must apply on all equipment connected to the network of Ens de Lyon.

- Any experimentation on the security of computer resources and networks, or computer viruses, without prior approval of the head of security (the RSSI) is prohibited.

- The user agrees not to access the information of other users on the network. They accept to be monitored following the use of email regarding some general indications of the exchanged message and not its content.

- The user may have personal Web pages for professional use. The content of these individual pages is made up by the user under his/her sole responsibility. He is the editor in the sense of the law No. 861067 of 30 September 1986. In the event where these pages obviously contain illicit content, ENS de Lyon reserves the right to suspend usage.

- When users are required to create files with such personal data as defined by the law of January 6, 1978 relative to computers, files and personal liberties, they shall ensure in particular:
    - to respect the procedures with the national commission for computing and liberties (CNIL);
    - to carry out prior information checks on the persons concerned as to the purpose and the recipients of the processing of this information;

Respect of rights:

Respect for intellectual property:

Users must refrain from copying, distributing or reproducing any software or document protected by copyright law. In general, users ensure that what they broadcast on the Internet or data they download does not affect the rights of third parties (copyright, right of brands, right to respect of privacy, etc.).

Respect for the people's rights

It is forbidden for anyone to infringe on the privacy of others through any process, including the transmission without consent of their image or the dissemination of confidential or private written material. In general, the user ensures the respect of the person, privacy and the privacy of others.

Respect of contractual clauses

Users must notably respect contractual obligations concerning the use of electronic documentary resources and notably to use them in a reasonable, personal and strictly non-commercial way.

Correct behaviour

Users must not use the information system to harass other users with unwanted communication from third parties or to display/publicize any illegal information.

Control and traceability

The establishment is under a legal obligation to implement a logging system, archiving Internet access, messaging and exchanged digital communications. These journaling files (called "logs") are processed to improve the security of computing resources or detect misuse of the latter. These "logs" can be made available by judicial application.

These files contain information allowing the identification of the user, the data related to the equipment used, date, time and duration of each communication, data relating to the additional services requested or used and their suppliers, to identify the recipients. Logs can be kept for up to one year.

The establishment uses a system of "intrusion detection" which analyzes real-time network traffic and alerts the RSSI of any potential signs of a hacking attempt.

Continuous service, management of absences and departures

Users are responsible for their private data. Upon their departure, they must destroy their data. Business data must be stored on shared spaces: shared folders per department, or boxes per facility.

Protection of the personal data

Pursuant to the provisions of the data protection Act No. 78-17 of January 6, 1978 and the European directive 95/46/EC relating to the protection of personal data and the free movement of such data of October 24, 1995, the establishment is committed to respect the legal rules of protection of such data.

It guarantees including the user :

- to use personal data only for the purpose for which they are collected (opening of the account, technical controls..);
- to communicate the purpose and the destination of the information recorded and to specify until when they can be conserved, which cannot in any event exceed what is necessary to achieve the purposes for which they are collected.
- to ensure a right of access and correction to the data concerned.

Legal reminders

Users are required to comply with the legislation in force:

-the respect for people (not to breach privacy or secrecy of correspondence, insults or defamation) 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 Criminal Code, art. 432 - 9 modified by the law nº2004-669 of 9 July 2004, section 29 of the Act of 29 July 1881, section 26, 27,34, 36 of the law No. 78-17 of January 6, 1978, art. 313 1 and suite 323-1-323-7 changed by law No. 2004 - 575 of June 21, 2004, of the Penal Code;

-the protection of minors against degrading or violent content or encouraging their corruption; Article 227-24, 227-23 of the Penal Code, law 2004 - 575 of 21 June 2004;

-respect for public order, which condemns racism, anti-Semitism or the glorification of crime; Section 24 and 26bis of the Act of 29 July 1881, Article L 323 - 1 ets. of the Criminal Code;

-respect for the copyright of literary, musical, photographic or audiovisual works online, respect for intellectual property for software. Article L 335-3 L 111-1, L 121-1, 122-1, L 123-2, 131-2 of the Code of intellectual property.

-Protection against computer-related crime: unauthorized access on an automated system, destruction or modification of data, fraudulent introduction of data, obstructing the functioning; Act of 5 January 1988 called "Jacques Godfrain law" and its 7 items (323-1-323-7);

-Law of conservation of the data connection: "electronic communication operators retain the needs of research, finding and the prosecution of criminal offences: the information to identify the user, data of used communication terminal equipment, technical features, as well as the date, the time and duration of each communication, data relating to the additional services requested or used and their suppliers. data used to identify the recipient of the communication. "Decree No. 2006-358 of March 24, 2006 art. A. 10-13 - I;