**INFORMATION TECHNOLOGY CHARTER**

| Reference : extract- internal rules and regulations | | | |
|---|---|---|---|
| | Name | Position | Date and signature |
| Author | | | |
| Revised by | | | |
| Validation: | Bruno Frédéric | Head of IT Support Department | July 2012, 03 |
| Circulation: | | | |
| Observations | | | |
| File : Indformation_Technology_cherter.pdf | | | |

| Revised versions of Document | | |
|---|---|---|
| Version | Date | Modifications made |
| 1.0 | 14/10/2009 | Extract from internal rules and regulations |
| 2.0 | 2/11/2010 | Updated rules and regulations |
| 2.1 | 10/juil/2012 | English Version |
| | | |
| | | |



## ARTICLE 33. RULES AND REGULATIONS FOR THE ACCESS OF INFORMATION SYSTEMS

### 33.1 Rules and Regulations Concerning the Correct Use of Information Systems and Networks

The current chapter aims to define the rules and regulations of use of the establishment's information systems, to remind the user of their obligations and to advise the user that this activity falls within a precise legal framework including criminal sanctions.

#### 33.1.1 Scope

The following rules, regulations and obligations apply to any person using the information systems of the school: user, teacher, student, research-lecturer, researcher, administrative or technical personnel, doctoral candidate, intern…

The rules and regulations defined cover the use of the following resources:

-software and equipment (servers, workstations, micro-computers and their associated peripherals), situated in the administrative services, classrooms, multimedia rooms and laboratories of the school,

-the establishment's networks and external networks (RENATER and the INTERNET, the DGA network) accessible through the intermediary of the school's networks.

The use of the school's networks and RENATER is strictly reserved for the purposes of training, teaching, research and professional use. The use of the RENATER network is also governed by the "Acceptable Use Policy" which the establishment has undertaken to respect.( http://www.renater.fr/IMG/pdf/charte_en.pdf)

The user is personally responsible in the case of non-respect of the rules and regulations. The establishment is, itself, subject to the rules and regulations governing information systems, and as such, must ensure the respect of codes of practice and the law.

The use of the Internet notably via the school's network or RENATER is controlled: all downloading of multimedia material (video and audio) is forbidden.

### 33.1.2 Authorization of Access to Resources

To use the information technology resources at the school, prior permission must be sought via a request to open a user account.

This authorization is strictly personal and cannot be transferred, even temporarily, to a third party.

The information technology systems of the school can only be used for the purposes of education, research and management. Any use for externally-financed project or study contract must be authorized by the school's director and the Information Technology Support Department. Private, non-abusive use of the information technology systems respecting the rules and regulations is tolerated (the Internet, File Transfer, email).

The account holder must provide correct personal data. He is also under obligation to inform the Systems Administrator of any changes to this information. The school reserves the right to withdraw authorization at any moment and without prior warning.

## 33.2 Rights and Obligations of the User.

### 33.2.1 Basic Principles

The user is responsible for his use of the school's information technology systems.

On a personal level, he must therefore ensure security. In particular:

- He must choose secure passwords, respecting the recommendations of the Systems Administrator. These passwords must be kept secret, must not be written down and must never be communicated to a third party. Upon the request of the Systems Administrator or OSSI, they must be changed at least once a year.

- - He is responsible for his files, directories and the access he grants to other users for the purposes of reading and modification.
- - He must not use accounts other than those he has been authorized to use. He must refrain from any attempt to acquire or decode the password of another user. He must refrain from any falsification of identity.
- He must not actively use or develop any programs endangering the information technology systems of the school or the national and international networks.
- He must inform the school Systems Administrator of any concrete violation, attempted violation or suspicion of violation of the information technology systems.
- He must log out before leaving a computer.
- He must not add or connect IT equipment to the local network without implicit authorization (examples of which being access in the Student Hall of Residence or wifi using “invité”) or explicit authorization.
- He must respect the procedures and instructions of the Systems Administrator.
- He must inform the Head of Information Technology of the school if he detects any gaps in the security system or any malfunctions.
- He must take the necessary precautions to avoid introducing a virus into the information technology systems, thus he must be vigilant and activate the protection tools at his disposal (for example : the anti-virus program) notably upon each file download or copy.
- He undertakes to use the available resources correctly (computers, printers etc) and not to overload the memory, disk space, network bandwidth…..for example: not to use the “diffusion générale” or “broadcast” email function for documents and images when unjustified.
- He undertakes to respect the available equipment such as : the UNIX workstations, personal computers, portable computers, printers etc

**33.2.2 Respect of Intellectual Property**

According to the general principle laid down in Article 20, the reproduction of commercial software other than for the purposes of a back-up copy, is strictly forbidden.

Prior authorization must be obtained, before any installation of commercial software on the school’s information technology systems ,through a Software Authorization Request. After authorization has been granted, the software is installed by the Information Technology Support Department.

For software in the public domain, the associated copyrights must be respected. For any document (books, articles, images, sounds….etc) the user must abide by the associated copyrights.

**33.2.3 Respect of the Confidentiality of Information.**

The user must:

- Not attempt to read, copy, disclose or modify the files of another user without explicit authorization,
- Refrain from all attempts to intercept communication between third parties (electronic mail or direct conversation),
- Adopt the data protection measures undertaken by the school to third parties guaranteeing the respect of confidentiality commitments,
- Protect the confidential data for which he is responsible and which he uses or records on the material means at his disposal such as: hard drives (local or network), USB flash drives (memory sticks) etc

**33.2.4 Respect of Individual Freedom**

Prior authorization must be obtained from the Commission Nationale de l'Informatique et des Libertés (C.N.I.L.) before the creation of any file containing personal information.

The information communicated through the school systems and networks must not breach an individual's right to privacy, or damage his image , or advocate racism, anti-Semitism or xenophobia.

**33.2.5 Connections with Other Information Technology Sites.**

It is forbidden to connect or to attempt to connect to another site without official authorization.

It is forbidden to use the school systems to commit acts knowingly endangering the security of other sites and telecommunications networks.

**33.2.6 Regulations Governing Electronic Communication**

During electronic communication, no one may write on school behalf or commit the school without prior authorization. No one may usurp the identity of another person at the school.

**33.3 Supervision and Monitoring**

The Systems Administrator:

-is the only person authorized to install and manage the equipment, except in exceptional cases . He ensures the correct functioning of the information systems of the school and sees that the rules ,regulations and codes of good conduct and correct use of those systems are respected.

-is bound to observe professional secrecy and confidentiality, and is invested with all the powers , for necessary investigations, for ensuring that the systems are used correctly. He will reserve however this action for the only cases required by the correct operating and the security of the systems. He undertakes not to disclose the information acquired during his investigations.

- can explore the users' files and report extracts to the Management if such an investigation is necessary due to the non-respect of the afore-mentioned rules of access to the resources,

-can also generate and consult an event log, and record traces if necessary.

In application of the Law of 23 January 2006 relative to the fight against terrorism and the Decree of 24 March 2006 relative to the conservation of electronic communication data (Reference 15), the information Technology Support Department of ENSTA Bretagne has at its disposal the technical means of monitoring electronic communication : electronic communications operator under the terms of Article L34-1 (I and II) of the Code des Postes et des Communications Electroniques (Reference 16), ENSTA Bretagne must, when necessary for the purposes of research, investigation and prosecution of criminal offenses, conserve the data relative to communications under the conditions stipulated in Article R10-13 of the Code des Postes et des Communications Electroniques (Reference 13).

**33.4 Implementation Procedures**

The procedures for access to the information resources can be consulted in the internal reference document of ENSTA Bretagne.

**33.5 Applicable Sanctions**

All users who have not respected the dispositions in the present Article will be subject to the school sanctions (see Article 3 supra), and/or civil or criminal prosecution under the Laws of the Republic (References 18 to 22).

**Reference Documents**

15) Law n°2006-64 of 23 January 2006 relative to the fight against terrorism, consolidated version 3 December 2008, and Decree n° 2006-358 of 24 March 2006 relative to the conservation of electronic communication data, consolidated version 23 December 2006;

16) Article L34-1 (I and II) of the Code des Postes et des Communications Electroniques (the Post and Electronic Communications Code);

17) Article R10-13 of the Codes des Postes et des Communications Electroniques (the Post and Electronic Communications Code) ;

18) Loi n° 78-17 of 6 January 1978 relative to information technology, files and freedom, consolidated version 14 May 2009,

19) Law n° 2006-961 of 1 August 2006 relative to authors' rights and related rights in an information society, consolidated version 3 August 2006;

20) Law n° 94-102 of 5 February 1994 relative to the repression of counterfeiting and modifying certain dispositions in the Code de la Propriété Intellectuelle (the Intellectual Property Code) , consolidated version 8 February 1994;

21) Law n° 94-361 of 10 May 1994 concerning the implementation of (E.U.) Directive n° 91-250 of the European Council dated 14 May 1991 concerning the legal protection of computer programs and modifying the Code de la Propriété Intellectuelle (the Intellectual Property Code) consolidated version 11 May 1994;

22) Law n° 90-602 of 12 July 1990 relative to the protection of persons against discrimination due to their state of health or their handicap, consolidated version 4 August 2006;