CHARTER FOR THE USE OF IT AND DIGITAL RESOURCES AT CENTRALE NANTES

1. Preamble

As referenced in the school rules and regulations, the school's IT Charter aims to:

- define the rules for the use of school IT resources;
- define the rights and duties of users, as well as of the school, as the resource provider;
- make users aware of IT security issues.

Each user of an IT resource or service provided by the school agrees to comply with this charter.

Should the IT Charter be updated, users are notified by email and are deemed to tacitly accept all updates.

2. Definition of terms: “IT resources", "User" & "IT account"

The term "*IT resources*" refers to all fixed and mobile computer hardware equipment (computers, tablets, telephones, printers, etc.), all software, support and application systems, as well as all network services and devices (Wi-Fi, Ethernet, box, cloud, etc.) deployed by the school.

The term "*user*" is defined as: - any member of permanent staff of the school, - any authorized member of staff of the companies incubated in the Centrale-Audencia-Ensa incubator, - any student enrolled in the school, - all temporary staff explicitly authorized by school management.

Each authorized user has a personal “*IT account*”, with associated access rights (applications, services, shared folders, etc.).

Signature of this charter is a prerequisite for the creation of an IT account.

To log in to his/her account, the user must enter:

- an identifier: assigned by the school to the user;
- a password: that the user chooses and can change independently;

This information must be entered to access IT resources. In some cases, identifiers are not required because they are already stored in the application which the user is accessing securely.

3. Access to IT resources

Network-connectable IT resources can be interconnected by the school's network, which is itself securely connected to the Internet.

The user can thus access resources according to the rights linked to his/her IT account, via the school’s internal network (Ethernet or Wi-Fi), or via an external Internet connection (if necessary via a VPN). The connection can be established either via standard or fibre optic broadband or via the "3G/4G" telecommunications network.

The provision and use of mobile equipment belonging to the school (mobile phones, laptops, etc.) is subject to a specific charter.

4. Use and safety regulations

The school's IT resources must be used in a rational, fair and reasonable manner, in compliance with the recommendations set out in this charter and with French legislation.

All users are responsible for their use of IT resources and networks to which they have access, and must contribute to the school’s general security. Each user:

- must respect the integrity and use of the resources made available by the school, and must in no way damage them. Any operational problems should be reported to IT;
- may only use the account(s) which he/she has been authorized to use. In no event should access codes be shared with a third party. The user is prohibited from using any computer account or access codes other than his/her own. Identifiers and passwords must not be communicated to anyone, including school departments. NB: troubleshooting does not require the user's password to be divulged;
- carefully chooses his/her passwords: easy for the user to remember, but difficult for others to guess, (see recommendations and good practice: https://www.ssi.gouv.fr/guide/mot-de-passe/);
- closes his/her workstation during any absence, so as not to leave resources or services accessible to a third party;
- is personally responsible for any operation carried out using his/her access codes.
- is aware that only the computers managed by the IT team are regularly backed up. The user him/herself is responsible for safeguarding data on computers not managed by the IT team;
- reports any anomaly or breach - real, attempted or suspected - of a computer system to the administrators of the affected equipment, as well as to the IT team, the RSSI (IT System Security Officer: rssi@ec-nantes.fr) and the FSD (Defense Security Officer: fsd@ec-nantes.fr);

- is informed that IT User Support is the sole point of contact for any request concerning account creation or deletion, data deletion, or e-mail quota, etc. Fraudulent messages – which often impersonate messages sent by IT departments - are routinely sent by hackers attempting to steal user data. If in doubt, users must contact IT user support (svp-dsi@ec-nantes.fr). Do not click on unknown links.

The following rules apply to equipment that is not managed by the IT team:

- any connection to the school's network via personal equipment or equipment non-identified by IT must be authorized by the IT team or the relevant laboratory, who may, for this purpose, seek advice on the user's authority. Once this authorization has been obtained, the user agrees to keep his/her system up-to-date and to configure it according to the rulebook. In particular, he/she must comply with school rules, especially with regard to combatting viruses and computer attacks. These rules are available on the school Intranet;
- if the user's activity requires the installation, download or use of specific software not provided by the school, he/she must first ensure that the associated license fees have been paid, that the download site is trustworthy, and then obtain permission for those downloads from IT or the relevant laboratory. IT can only install software on equipment that it manages.

5. Regulations concerning the use of the school's IT resources for personal use

The school's IT resources are intended for professional use. As such, school equipment should be used to produce material, accomplish tasks or consult information for professional purposes only.

However, a reasonable degree of personal use of messaging, file storage, telephone and Internet access via school resources is tolerated, as long as it does not adversely affect school operations, the integrity of its IT network or the activity of school employees.

Any message sent or received from professional email is assumed to be of a professional nature unless it is clearly identified as personal by the user. To be identified as personal, a message must be saved in a folder marked 'PRIVE-PRIVATE'.

All files on a work computer are assumed to be of a professional nature unless clearly identified as personal by the user. To be identified as personal, documents must be saved in a folder marked 'PRIVE-PRIVATE'.The title "My documents", the initials or the first name of the user are not enough to identify files as personal.

6. Obligations relating to confidentiality

- any attempt to intercept communications between third parties is prohibited;
- the user only has access to publicly available information or files, as well as his/her own information or files. It is forbidden to read information or files reserved for the use of other users, even if these elements are not protected. Any breach of the present obligation may lead to legal proceedings against the perpetrator;
- the user is bound to discretion and professional secrecy in regard to any information relating to the internal workings of Centrale Nantes and its IT resources;
- the user is required to take the necessary data protection measures required to respect confidentiality commitments made by Centrale Nantes vis-à-vis third parties;
- the institution's Intranet is intended for the dissemination of information internally.

7. Obligations relating to intellectual property

The use of any software (source or binary code) and more generally any document (file, image, sound, etc.) must comply with the intellectual property law, the recommendations set by rights holders and the commitments made by Centrale Nantes (licensing agreements for example). In particular,

- it is strictly forbidden to make copies of commercial software for any use whatsoever, except a backup copy under the conditions provided for in intellectual property law;
- software can be installed only in compliance with the legislation in force, with the author's and the publisher's recommendations, and with the IT team's recommendations. It is also subject to payment of the rights of use;
- It is forbidden to circumvent restrictions on software use.

8. Analysis and control of IT resource use

For legal and security reasons, as well as maintenance and technical management needs, data for the use of hardware, software and network resources is saved in files which are stored and archived and kept for their regulatory periods. This data can be exploited to determine the origin of a malfunction, malicious behavior or misuse.

The procedures implemented comply with French and European legislation, including the GDPR (General Data Protection Regulation) and decisions applying since the law n ° 78-17 of 6 January 1978 relating to data processing, computer files and freedoms.

9. Personal data

School provisions concerning the application of the GDPR (General Data Protection Regulation) are made available to all users of the school, and are published on its Intranet.

10. Systems Administration

Hereafter, the term "systems administrator" refers to a person who is responsible for the upkeep, configuration, and reliable operation of the computer systems, hardware and software (tools, networks, databases, messaging, etc.) of the institution or of the entities that make it up.

The role of a systems administrator is to ensure that the computer system resources under his or her responsibility, including servers, network equipment, security equipment, applications, databases and workstations, work properly and securely.

In the course of his/her duties, the systems administrator has technical access rights that may allow him/her to access information, such as e-mails, files, connection data (confidential or not), and in general to data of a private or professional nature, of which he/she is neither the recipient, nor the author, nor the owner.

The systems administrator is bound to discretion and professional secrecy. He/she shall undertake his/her duties in compliance with the regulatory provisions governing his/her status, thus excluding any use of his/her access rights for personal reasons. Similarly, he/she shall not use his/her rights to transfer data for which there is a procedure in place, and thus replace the entity in charge of the data.

Systems administrator rights

Within the framework of his or her duties, a systems administrator has the right to:

- interrupt the operation of any equipment, software or hardware that would compromise the security or proper functioning of the computer systems;
- use connection data (which may involve the discovery of private information) for diagnostic, verification, metrological or statistical purposes or in the event of an anomaly or incident
- to intercept or prohibit any IT flow (web, e-mail, file transfer, telephony, video, etc.) that presents potential security risks (viruses for example), or that contravenes the present IT charter;
- to take appropriate measures to prevent any security risk such as viruses, intrusion or theft of data, destruction of data or circumvention of the security policy.

Systems administrator duties

Within the framework of his or her duties, a systems administrator:

- does not knowingly access user data identified as personal - except on a case-by-case basis, with the formal agreement of the user him/herself - and does not authorise anyone to access it, except in specific cases provided for by law
- scrupulously respects the confidentiality of the information to which he/she has access and implements measures to ensure that it is not disclosed;
- works with the Data Protection Officer (DPO) to ensure that the implementation of processing operations complies with the regulations on the protection of personal data. He/she contributes to the availability, confidentiality and integrity of the data concerned and alerts the DPO of any incident in this regard;
- works with the other systems administrators so that all information is processed in accordance with this charter
- informs the Information Systems Security Manager of any security incident of which he/she becomes aware;
- uses his/her access rights exclusively for activities and needs directly related to his/her duties, and under no circumstances for personal reasons;
- acts in the interests of better security and in the interests of the institution.

Systems administrator obligations

The systems administrator undertakes to respect the legislation in force and the internal regulations of the institution in all circumstances, including the provisions of this charter. In the event of non-compliance, the systems administrator will be held responsible for his/her actions and may be subject to disciplinary, civil or criminal proceedings.

11. Business continuity in the event of employee absence

In the event that an employee is unable (for example, in the event of sick leave) to provide the information he/she has at his/her disposal or to which he/she has access on computer systems, which is necessary for continuity of the establishment's activities, the director of the establishment may, exceptionally, authorise access to this information or computer systems by named persons, under strict supervision. This authorisation, made formal in writing and brought to the attention of the employee whose absence is likely to disrupt business continuity, shall include the following elements:

- identity of the absent employee;
- reminder of the context (sick leave of the employee, etc.);
- data or systems accessed;
- purposes under Article 6.1.e of the GDPR;
- scope of data accessed (e.g. access to work-related messages only);
- list of names and functions of the persons having this access;
- mandatory presence of the DPO (Data Protection Officer);
- period(s) during which such access is authorised.

A report will be drawn up, and made available to the employee, in which the procedures for these consultations, the elements consulted and, where appropriate, the actions taken will be recorded.

12. Compliance with legislation

All users must comply with all applicable legislation, particularly in the field of IT security and personal data. These texts are constantly updated and can be consulted on the websites of the CNIL (www.cnil.fr) and LEGIFRANCE ((www.legifrance.gouv.fr), which publishes most French laws free of charge.

13. Disciplinary action

Any infringement of this charter or the regulations in force may lead to the suspension or permanent withdrawl of access rights authorized by the school. Failure to comply with any of these rules may result in disciplinary action within the institution.

Anyone who breaks the law is liable to prosecution. Users are reminded that their actions may have serious legal consequences as a result of unauthorized behaviour.

*****

I, the undersigned,

FIRST NAME and Surname: ____

declare that I have read this "Charter for the use of IT and digital resources at Centrale Nantes" and I agree to comply with the rules herein. I am aware that if I infringe these rules, Centrale Nantes may cancel my access to its facilities, without prejudice to any legal proceedings that may be brought against me.

Administrative Department / Laboratory / Teaching Department / Other:

____

Date: __________/___________/________

Signature: