



Charter Defining the Use of IT Facilities

**Institut polytechnique de Grenoble,
Graduate Schools of Engineering and Management,
Université Grenoble Alpes**

Index

Preamble	3
Article I. Scope	3
Article II. Right of Access to IT Facilities.....	4
Article III. Data protection and privacy	4
Article IV. Conditions of Use of IT Facilities	4
Section IV.1 Professional vs. Private Use	4
Section IV.2 Maintenance of Departmental Operations in Case of Absence and Departure.....	5
Article V. Security principle.....	5
Section V.1 Applicable Security Rules	5
Section V.2 Notification Obligations	6
Section V.3 Control and Monitoring Policy	6
Article VI. Electronic Communication	6
Section VI.1 Emailing.....	6
(a) Email Addresses	6
(b) Email Content.....	7
(c) Sending and Receiving Emails	7
(d) Legal Status of Messages.....	7
(e) Storing and Archiving of Messages.....	7
Section VI.2 Internet	7
(a) Publication on Establishment Websites or Intranets.....	8
(b) Security Policy.....	8
Section VI.3 Downloading Policy	8
Article VII. Traceability.....	8
Article VIII. Compliance with Intellectual Property Rights	8
Article IX. Compliance with Data Protection Act	9
Article X. Limitation of Access	9
Article XI. Charter Commencement Date.....	9
Appendix	10
Core Legal References.....	10
(a) Offences under Nouveau Code Pénal (New Penal Code).....	10
(b) Press Offences (Loi 29 juillet 1881, amended)	10
(c) Intellectual Property Code Infringements.....	10

Preamble

The following translation is for information only and has no contractual value.

The phrase 'IT facilities' refers to all the data, hardware, software, applications, databases and local telecommunication network resources, as well as all resources which enable remote or transitive access from the network of Institut polytechnique de Grenoble, Graduate Schools of Engineering and Management, Université Grenoble Alpes.

It also encompasses mobile computing facilities, such as personal digital assistants, portable computers and mobile phones.

The term "user" refers to any person entitled to a computer account or having access to the IT facilities regardless of status.

Notably, this refers to:

- *Any staff, irrespective of his or her contract, fulfilling an assignment coming under the provision of public service in the fields of teaching or research;*
- *Any student enrolled in the Establishment;*
- *Any person exterior to the Establishment, visitor, guest, or person under contract¹ to the Establishment.*

Proper operation of the IT facilities requires compliance with the legislative and regulatory requirements, notably compliance with rules concerning security, operation procedures and data storage.

This chapter defines the rules of use and security with both the Establishment and user agree to comply with. It specifies the rights and duties of each party.

Responsibilities of the Establishment

The Establishment must inform the user of the charter.

The Establishment must take all necessary measures to ensure the security of the IT facilities and the protection of users.

The Establishment must facilitate user access to the resources available via the IT facilities. Although the resources available are for professional usage the Establishment must respect the residual use of IT resources in a personal capacity.

Responsibilities of the User

The user is responsible, at all times, for the usage which he or she makes of the available IT facilities. He/she has an obligation of confidentiality with regard to the information and documents he/she produces or accesses. This responsibility implies the respect of rules concerning professional ethics and confidentiality.²

In any case, the user shall comply with the requirements associated with his or her position or contract.

The available resources must be used appropriately and in good faith so as to avoid hindering the performance of the IT facilities and abusive use of resources for personal ends.

Article I. Scope

The security rules and terms of use defined in the Charter apply to the Establishment and all of its users.

The use of IT facilities related specifically to the activity of union organisations is not covered by the Charter.

¹ Compliance with the Charter must be explicitly stated as an obligation within the contract.

² In particular, patient confidentiality in health related fields.

These rules apply to any person authorised to use any of the computer facilities of the Establishment, including off-site and shared computer facilities, and covers external networks accessible through Establishment networks.

Article II. Right of Access to IT Facilities

Right of access to IT facilities is temporary. Access will be withdrawn if no longer justified by the situation of the user and, unless specifically requested, will be withdrawn within 3 months of the expiration of a user's computer account entitlement.

It may also be withdrawn, as a precautionary measure, if the behaviour of a user is incompatible with the rules as specified in the Charter.

Article III. Data protection and privacy

The user is responsible for his or her professional data, or that to which he or she has access in the scope of his or her duties. In particular, he/she must ensure that his/her data are backed up and that he/she is vigilant about the access rights it gives to other users.

The user must ensure the protection of sensitive information (for which a direct or indirect requirement for confidentiality has been identified); in particular, he/she must avoid communicating or transporting it without protection (encryption) via insecure media (messaging, USB keys, laptops, external disks, etc.) and must not place it on a external server or available to the general public.

Article IV. Conditions of Use of IT Facilities

Section IV.1 Professional vs. Private Use

Use of the IT facilities of the Establishment exclusively covers purposes of research, teaching, documentation, administration or other aspects of university activity. Unless authorised, these systems cannot be used for the operation of projects which are not associated to the Establishment or to projects assigned to the user. They may, however, be used for private communication under the conditions described below.

Residual usage of the IT facilities for private use must be for non-profit activities and moderate in terms of frequency, volume and duration. Whatever the case, the additional resulting costs must be negligible in comparison to the overall operation costs.

This usage must not have a negative effect on the quality of work provided by the user, on the time the user dedicates to his or her working duties or to the proper functioning of the Establishment.

All information is considered professional with the exclusion of data explicitly designated by the user, as relative to his or her private life, regardless of the medium (computers, USB sticks, phones, etc.) or the service used (storage space, messaging, etc.).

Thus, it is the responsibility of the user to store data of a private nature in an appropriate area dedicated explicitly³ for this purpose or to indicate the private nature of the data on the resource⁴. The user is responsible for the protection and backup of private data.

The user is responsible for his or her private data space. Upon his or her departure from the Establishment, it is his or her responsibility to delete his or her private data space. The Establishment does not have the duty to maintain this space. Data conservation measures of professional data are defined by the person deemed responsible by the Establishment. In the case of the death of a user, his or her private space will be deleted.

Private usage of the IT facilities must respect the applicable laws.

In particular, the storage, dissemination or exporting of images of a paedophile nature, or the

3 For example, this space may be named "_private_" or "_prive_"

4 For example, "_private_name_of_object": the object may be a message, a file or any other digital resource.

dissemination of anti-Semitic or racist material⁵ is strictly forbidden.

Additionally, in character with the aims of the Establishment, consultation of sites of a pornographic nature within the grounds of the Establishment, outwith a professional context, is forbidden⁶

Section IV.2 Maintenance of Departmental Operations in Case of Absence and Departure

In order to maintain departmental operations, the user should make every effort to store files in the areas shared by the members of his or her department or work group. In any case, any data not situated in the space identified as private will be considered as belonging to the Establishment that will be able to have unrestricted access.

In the case of departure or prolonged absence, the user must inform his or her hierarchy of the procedures allowing access to the resources made specifically available to him or her. These procedures shall comply with the safety rules set out in Section V. 1.

Article V. Security principle

Section V.1 Applicable Security Rules

The Establishment will take appropriate security measures for the IT facilities available to users.

The user will be informed that access codes constitute one of the security measures aimed at avoiding malicious or abusive use. However, this security measure does not imply that information tools protected in this way are of a personal nature.

The levels of access granted to the user depend upon the tasks assigned to the user. The security of the IT facilities available requires that the user:

- Follow the security instructions, notably the rules relating to the management of access codes. Each user is responsible for the usage made of their access codes.
- Keep his or her access codes confidential and never share them with a third party.
- Respect the access policy, and in particular, not use the access codes of another user nor attempt to attain them.
- Ensure that he or she never leaves a freely accessible work station unattended.

In addition, the security of the resources available to the user requires several precautions:

- ✓ On the part of the Establishment:
 - Ensure that sensitive information is only accessible to the persons concerned. Exceptions may be made for practices concerning organisation of departmental operation continuity, as decided by the relevant hierarchy.
 - Limit the access of the user to only the information for which he or she has been explicitly allowed.
- ✓ On the part of the user:
 - Ensure that he or she does not access or attempt to access resources available via the IT facilities for which he or she has not been explicitly granted permission.
 - Ensure that he or she does not connect devices directly to the local network other than those authorised by the establishment or those detailed in a user guide defined by a department or the Establishment.
 - Ensure that he or she does not install, download or use software without the required license or originating from untrustworthy sources or without the authorisation of the Establishment.

5 Article 24 and 26 bis of *Loi du 29 juillet 1881*.

6 *Code Pénal* (Penal Code), article L 323-1 and subsq. articles.

- Follow the guidelines defined by the Establishment concerning viruses and computer program attacks.
- Ensure that he or she does not intentionally jeopardise the smooth operation of the computer resources and networks by abnormal usage of hardware or software.
- Make all efforts to safeguard the equipment made available to him or her against theft or damage.
- Apply any security recommendations issued by the Establishment.

Section V.2 Notification Obligations

The user must notify the person responsible for the security of IT facilities of any irregularity, such as a security breach, as soon as possible. He or she must also notify his or her superior or the hierarchy of any access to a resource which does not correspond to his or her status.

Section V.3 Control and Monitoring Policy

The user shall be provided with the following information:

- Procedures for corrective, curative or adaptive maintenance. The establishment reserves the right to perform maintenance (remotely if necessary) upon any resources provided.
- The user will be informed of any remote maintenance prior to its occurrence.
- Any information blocking the operation of IT facilities or causing disruption through its delivery, will be quarantined and if necessary deleted.
- The IT facilities, within the boundaries of the applicable legislation, may be subjected to the following: surveillance or testing measures for statistical purposes; traceability measures for legal or functional requirements; optimisation; security measures; detection of abusive behaviour measures.

The personnel responsible for the control operations of IT facilities are bound by professional confidentiality. They are not permitted to divulge any information which they may encounter as part of their functions given the following circumstances:

- The information is covered by correspondence confidentiality or, being identified as such, is private information of the user.
- The information does not jeopardise the proper operation of applications or their security.
- The information does not fall under article⁷ 40, paragraph 2 of the *Code de Procédure Pénale* (Code of Criminal Procedure).

Article VI. Electronic Communication

Section VI.1 Emailing

The use of emails constitutes one of the essential elements for work optimisation, the sharing of means and resources and the exchange of information within the Establishment.

(a) Email Addresses

The Establishment will provide the user with a nominative professional email address for sending and receiving email. Once assigned, use of this nominative address will be under the responsibility of the user.

This nominative email address is merely an extension of the administrative address and does not diminish the professional nature of the messaging system in any way.

⁷ The obligation of every civil servant to notify as soon as possible the *Procureur de la République* of any crime or misdemeanour of which he or she becomes aware as a result of their employment.

An email address related to a position or organisation-entity, can be created for a user or group of users when required by the Establishment.

The management of email addresses corresponding to institutional mailing lists designating a category or group of "users" is the exclusive responsibility of the Establishment. Such lists can only be used by authorised users.

(b) Email Content

Every message will be considered as professional unless explicitly referenced as being of a private nature⁸ or stocked in the private data storage area.

In order to maintain correct departmental operations, limitations may be implemented. In particular, reduction methods for undesirable messages (such as spam and viruses) may be put in place.

Messages containing content of an illicit nature are forbidden. Notably, this applies to content that contravenes the legal regulations on the freedom of expression and privacy (such as, jeopardizing an individual's peace of mind through threatening behaviour or defamation, damaging an individual's honour through non-public personal insult and breaches of copyright or the proprietary rights of a business).

All forms of electronic exchange (email, forums, etc.) must respect the accepted forms of normal behaviour applicable to any type of exchange, whether written or oral.

The transmission of classified data⁹ is forbidden without specific authorisation and the transmission of sensitive data, when unavoidable, must be sent in an encrypted format.

(c) Sending and Receiving Emails

The user must exercise vigilance regarding information received (disinformation, computer viruses, scams, chain letters, etc.).

The user must verify the identity and correctness of the address of a potential recipient of a message.

The user must ensure that the diffusion of messages be limited only to those concerned by its contents so as to avoid mass mailing, over-encumbered email accounts and an overall degradation of service.

(d) Legal Status of Messages

According to the law, digital writing has the same probative value as paper-based writing, so electronic messages exchanged with third parties can legally represent a contract.

The exchange of emails with third parties can, from a legal point of view, represent a contract, under the conditions specified in sections¹⁰ 1369-1 to 1369-11 of the *Code Civil* (Civil Law Code).

Consequentially, the user must attach the same importance to the nature of electronic messages as to traditional correspondence.

(e) Storing and Archiving of Messages

Each user must employ the necessary methods for the conservation of messages which may be indispensable or even merely useful as evidence of a particular activity.

Section VI.2 Internet

It should be noted that the Internet is subject to the totality of applicable law. Use of the Internet (and by extension the intranet) is one of the essential elements for work optimisation, sharing and information accessibility within and outwith the establishment.

The Internet is made available as a work tool for professional purposes (administrative, pedagogical or research). Residual private usage, such as defined in section III.1, may be tolerated but it should be noted

8 For example, messages containing the terms ("private" or "prive") in the subject of the message.

9 This term refers to classified defence data which covers *confidentiel défense*, *secret défense* and *très secret défense* data.

10 Articles 1366-1367 of the Civil Law Code (Ordinance n°2016-131 of 10 February 2016 - art. 4)

that connections established using resources provided by the establishment are presumed to be of a professional nature.

(a) Publication on Establishment Websites or Intranets

Any publication of information on an Internet or intranet site belonging to the Establishment¹¹ must be approved by the person responsible for the site or the person, explicitly named, responsible for publication.

The publication of information of a private nature (such as a private site) using the IT facility resources belonging to the Establishment is forbidden, unless specifically authorised as defined in a user guide issued by the department or Establishment.

(b) Security Policy

The Establishment reserves the right to restrict or forbid access to certain sites and to perform surveillance, either before or after the fact, of sites visited and the duration of access.

Access is authorized solely in so far as it complies with the security procedures set up by the Establishment. Additional security procedures may be requested and defined in a user guide issued by a department or by the Establishment.

The user is informed of the inherent risks and limitations regarding use of the Internet through training and awareness programs.

Section VI.3 Downloading Policy

Any downloading or copying of files (notably sound files, images, software and online courses) on the Internet or locally must comply with intellectual property rights as defined in Article VII.

The Establishment reserves the right to limit the downloading or copying of certain files on the basis of file size or the possibility of security risks to the IT system (viruses, malicious code, spyware, etc.)

Article VII. Traceability

The Establishment is legally obliged to set up a data logging system¹² for Internet access, messaging and data transfers.

The Establishment reserves the right to install data tracking tools on all information systems.

The Establishment has adopted a "general policy for the management of computer logs", entered in the establishment's "informatique et liberté" register. It mentions in particular the conditions and the duration of conservation of the traces of connections or use of services, and the methods of expression of the right of access which the users have, in application of Act No. 78-17 of 6 January 1978 modified and of the European General Data Protection Regulation (GDPR - EU 2016/679).

Article VIII. Compliance with Intellectual Property Rights

The Establishment reminds all users that the use of IT resources¹³ implies the respect of its intellectual property rights, those of its partners and more generally, of all third parties holding such rights.

As a consequence, each user must:

- Only use software under the licensing conditions granted;
- Not reproduce, copy, distribute, modify or use software, databases, web pages, texts, images, photographs or other creative content protected by creative or exclusive rights, without having first obtained authorisation from the holders of these rights.

11 From utilising the IT resources made available to the user.

12 Storage of technical connection information such as access time, user IP address, etc.

13 Including pedagogical resources.

Article IX. Compliance with Data Protection Act

The user has the obligation to respect the legal provisions as regards automated processing of personal data, in accordance with the law n° 78-17 of January 6, 1978 known as "Loi Informatique et Libertés" (data Protection Act) and of the European General Data Protection Regulation (GDPR - EU 2016/679).

Personal data is information which – in whatever form – makes it possible to identify, either directly or indirectly, the physical person to whom it applies.

The creation of a file containing this type of information and related processing requests, including when they result from extraction, cross-referencing or interconnection of pre-existing files, are subject to legal obligations and must have been the subject of an instruction by the Data Protection Officer (DPO) of the Establishment.

In addition, in accordance with legal provisions, each user has rights relating to the data concerning him, including data relating to the use of information systems: information, consent, limitation, access, rectification, deletion, portability, right to be forgotten, breach notification, contestation of an automatic decision, right to compensation.

Exercises of this right may be handled by the Establishment's Data Protection Officer (DPO).

Article X. Limitation of Access

In the case of contravention of the regulations defined in this document and of the procedures defined in user guides established by departments or the Establishment, the "person legally responsible" for the Establishment may, independently of the legal or disciplinary actions that may be taken against the users, limit access as a precautionary measure.

"Person legally responsible" refers to any person with the capacity to represent the Establishment (university president, institute director, etc.)

Any abuse of resources made available to the user for ends outwith professional usage is open to sanction.

Article XI. Charter Commencement Date

This document annuls and replaces all previous documents or charters relating to the use of the Establishment's IT facilities.

It will be effective in each institution on the date of its approval by the competent authority.

It is an Appendix to the Rules and Policies.

Appendix

Core Legal References

(a) Offences under *Nouveau Code Pénal* (New Penal Code)

Offences against Natural Persons

Offences against personality: (Privacy rights section, art. 9, *Code Civil* -Civil Law Code)

- Offences against privacy (art. 226-1 paragraph 2 ; 226-2 paragraph. 2, art. 432-9 amended by *Loi n°2004-669 du 9 juillet 2004*); offences against the image of persons (art. 226-8)
- Malicious denunciation (art. 226-10)
- Breach of professional secrecy (art. 226-13)
- Violation of personal rights resulting from computer files or processes (art. 226-16 to 226-24, from *Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* and amending *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*)

Offences against Minors: (art. 227-23; 227-24 and 227-28).

- *Loi 2004- 575 du 21 juin 2004* (LCEN)

Offences against Property

- Fraudulent obtaining and similar offences (art. 313-1 and subsq. art.)
- Unauthorised access to automated data processing (art. 323-1 to 323-7 amended by *Loi n° 2004-575 du 21 juin 2004*).

Encryption

- Art. 132-79 (added to the Code by *Loi n° 2004-575 du 21 juin 2004* art. 37)

(b) Press Offences (*Loi 29 juillet 1881*, amended)

- Incitement to crime (art. 23 and 24)
- Condoning of crimes against humanity, condoning and incitement to terrorism, incitement to racial hatred, denial of crimes against humanity (art. 24 and 24 *bis*)
- Defamation and insult (art. 30 to 33)

(c) Intellectual Property Code Infringements

- Infringement of rights pertaining to works of the mind (software products included) (art. 335-2 amended by *Loi n° 2004-204 du 9 mars 2004*, art. 34 - and art. 335-3)
- Infringement of design rights (art. L521-4 amended by *Loi n° 2004-204 du 9 mars 2004*, art. 34)
- Infringement of trademarks (art. L716-9 – amended by *Loi n° 2004-204 du 9 mars 2004*, art.34 –and subsq. art.)

It should be noted that this list is for information only and subject to change.