

# **Charter for the use of IT and electronic communication resources of University Claude Bernard Lyon 1**

Considering the Education Code;

Considering the Intellectual Property Code;

Considering the Penal Code;

Considering the boards of directors' deliberation of University Claude Bernard Lyon 1 of November 26, 2002;

Considering the opinion of Structure Working Group of November 19, 2002;

Considering the opinion of Institution Joint Committee of October 24, 2002;

Considering the opinion of Scientific Council of October 21, 2002;

Considering the opinion of Studies and University Life Council of April 25, 2002;

Considering the opinion of board of directors of IT Resources Centre of November 14, 2002.

## **PREAMBLE**

PAGSI (French Governmental Action Plan towards Information Society) defined the dissemination of information related to public administrations and institutions by IT resources as the remit of public service.

Otherwise, the development of IT techniques involves a wider utilisation of electronic communication resources such as emails or discussion lists and forums.

The University Claude Bernard Lyon 1 is part of these goals by developing IT resources provided to students and staff of University in order to reinforce the initial and continuing training, promote research work and favour cooperative university work.

This charter defines the general terms and conditions of use of these services within the framework of activities related to goals and functioning of University. The uses that do not fall within this clear framework are tolerated. It aims to remind the effective texts and to regulate the functioning and use of university information system.

Information system means:

- All servers: computers or automatic telephone exchanges;
- All workstations and communication terminals: desktop or laptop computers, peripheral devices, landline or mobile phones;
- All transmission equipment: hubs, switches, router;
- The infrastructure of network link: microwave radio systems, optical fibre cables, UTP or FTP cables, equipment rooms;
- All software contained on or operating, inter-operating or protecting the aforementioned computers and IT materials, including communication protocols that enable:
  - o Constitution and creation;
  - o Exchange, circulation and dissemination;
    - Of data, files, databases,
    - Intranet, extranet,
    - Images, sounds, texts, programmes,
    - Any information flow

Between users between themselves or with external persons.

## **TITLE I – ACCESS TO INFORMATION SYSTEM**

### **Article 1 – Definition of user**

The user shall be the holder of an access account as defined in Article 3.

It deals, particularly, with students enrolled in an initial training or in the continuing training of University Claude Bernard Lyon 1, teachers, researchers and administrative, technical and health staff of University.

### **Article 2 – Definition of information system manager**

The person responsible of information system of University shall be defined as manager of information system. It may deal with several services. He shall ensure protection, maintenance, good working of information system and guarantee the respect of the present charter by all users and staff of IT services.

He shall ensure the execution of all necessary formalities and declarations, in particular the ones under the law n°78-17 of January 6, 1978 related to informatics, files, and freedoms and under the law of July 10, 1991 about the confidentiality of correspondence.

### **Article 3 – Access account**

The manager shall give one or several access account(s) on any equipment of University in order to favour the access to scientific information and to provide the sharing of knowledge and information related to specific goals of University.

This access account shall be at least realised to grant a username and a password strictly personal and confidential after written acceptance of the charter for user.

The identification of user shall be compulsory. The information that he gives shall be accurate and timely. If not, the opening of an access account could not be effective.

The user is responsible for operations made through his username and password; he cannot disclose them or appropriate the ones of another user.

### **Article 4 – Rights of users**

The access account shall give to user an annual right of access to services provided. This right of access is personal, non-transferable and temporary. It shall be subject to an annual renewal. It shall disappear as soon as its holder do not meet the award criteria defined in Article 1 of the charter.

This right of access can be adjourned at any moment, from the moment a failure to provision of the charter from user is supposed.

The user shall give expressly his consent for personal data concerning him to be collected within the framework of an access account opening. These data could only be used for enrolment purposes.

The user may ask to University the communication of nominative information concerning him and rectify them according the provisions of the law n°78-17 of January 6, 1978 related to informatics, files and freedoms.

The user shall be informed that in compliance with the effective laws and regulations, University shall be required to collect and keep information about users of its IT services and may be required to give them within a framework of an inquest.

Consequently, any refusal from user related to collecting personal information required shall involve a rejection of access account request.

## **Article 5 – Obligations of user**

The user shall undertake to inform immediately the manager of any loss, attempted violation or anomaly related to the using of his access account.

The user shall undertake to have a rational and fair using of services and, particularly of network, messaging service, IT and electronic communication resources in order to avoid saturation and misappropriation for personal purposes.

The user shall accept that University could know the information required to network administration (volumetry data, incidents, nature of generated traffic) and could take any urgent measures to stop disruption of its services. The University shall reserve the option, in particular, to stop the access to services in case of excessive or non-compliant using with its specific goals as defined in the present agreement.

The user shall be responsible for using the network. He shall guarantee particularly at his level, the security of this network and undertake not to bring deliberately any disturbance to its working and to jeopardise integrity of IT and electronic communication resources.

He shall undertake, particularly, not to:

- Stop the normal operation of network and connected systems;
- Develop, install or copy programmes dedicated to bypass security, fill resources;
- Introduce virus programmes or that bypass software protection;
- Install software likely to modify machine configuration without the prior agreement of manager;
- Prey on information systems of university or any public or private, European or foreign organism, and modify or alter the contents;
- Collect or intent to collect information likely to be used during attempted attacks against external or internal information systems;
- Use IT and electronic communication resources in order to duplicate, disseminate or distribute software, images, sounds and videos with contents under the penal code or collected by means that flout the intellectual property right, in any form.

## **Article 6 – Service availability**

The University shall endeavour, to the extent possible, to keep accessible the service that it proposes on a permanent basis but it is not bound by any obligation to manage it. The University may stop the access, particularly for reasons of maintenance, updating or security without being held responsible for consequences of these interruptions with regards to users or a third party.

## **Article 7 – Control and maintenance by the manager**

The user shall be informed that the manager may have an access to all components of the information system, except messaging service and personal spaces, at any moment and in order to operate any protective action towards information system concerning:

- Retaining and backing-up, control of absence of non-authorized dissemination of information on websites;
- Evidence of creation and dissemination date of the aforementioned information;
- Research and reject of intrusions in information or material system, breaking the rules related to copyright;
- Updating, maintenance, correction and repair of materials and softwares.

Should a component of information system could not be situated on University, the user who is in possession of it shall have to return it or entrust it to the manager on first demand from the latter.

The manager could implement tools of control and surveillance that meet the purpose to protect information system.

To this end, the University shall have the following technical means to proceed to the control of using of its services:

- Limiting access to proxy server;
- Firewalls;
- Intrusion detection systems;
- Metrology server.

Any user may obtain from manager, information on the implemented control means.

Technical controls that may be operated shall be justified in the interests of network security and/or IT and electronic communication resources:

For maintenance and technical management necessities, the use of services, and particularly material and software resources, as well as the exchanges via network, shall be analysed and controlled in compliance with applicable regulation and particularly in compliance with the rules related to private life. The University shall reserve the right, within the framework of these provisions, to keep the necessary information for the good system operation.

The manager shall also be in right to check, on the only Internet services, except for messaging service, that the disseminated contents remain consistent with the goals of University.

The board of director of IT Resources Centre (CARI for *Conseil d'Administration du Centre de Ressources Informatiques*) shall endeavour to respect of effective rules from both users and services that depend on manager. In particular, CARI could be submitted, as soon as a risk or statement of infringement to the rights of persons or to individual freedoms could be raised but that could not be justified by the nature of the task to achieve, nor proportionate to meet this aim. Besides, CARI could give its opinion in case of question raised by staff of IT Resources Centre on the responsibilities incurred within the framework of its interventions.

CARI shall report annually its activity to the board of director of University.

Technical services may have to perform backups, including on personal contents, in the exclusive goal to avoid information loss. These contents shall not be accessible to third parties, except legal proceedings.

## **Article 8 – Antivirus**

The University shall have an antivirus. Each user shall respect the instructions of Administrator regarding antivirus updating.

Only the manager shall be authorised to introduce new materials and software into information system. In case of expressed need from user for new material or software, he shall ask to Administrator prior authorisation.

The non-respect of these provisions may expose the user to sanctions and risk his liability in case of intrusion, because of user, of virus or third party non-authorized in the information system or in case of data losses.

## **Article 9 – Firewalls**

The University shall make CARI responsible for defining its security policy.

It shall have firewalls to protect its network. This equipment shall aim to limit some traffic depending on protocols used, either depending on ports, or depending on IP addresses. The manager shall define the rules of filtering to implement in order to guarantee an optimal security level, taking into account the rules set by CARI. Any user could make a written and reasoned request to modify rules to the manager. The manager could therefore follow it up if this request is consistent with University policy. In case of emergency, the manager can take provisional measures, which shall be subject to CARI validation afterwards.

## **TITLE II – USE OF INTERNET SERVICES**

### **Article 10 – Provided Services**

The University shall offer to user, in accordance with its technical capacities, an access to the Internet with the chance to navigate on the Internet network as a whole.

The available services on University website could particularly be constituted of:

- An area for educational and scientific information;
- An area for administrative information;
- A service of creation and hosting for personal pages;
- A service of electronic messaging (Title III of the present agreement);
- A service of forums;
- A service of online discussions;
- A mailing list.

### **Article 11 – Technical capacities**

The University shall equip itself with means that enable it to be an Internet service provider.

The University shall equip itself with means that enable it to be a Web site hoster.

The University shall equip itself with means that enable it to take part into provision of provider services reserved to higher education institutions.

The access to provided services may take place:

- Either from University sites (servers, self-service micro-computers);
- Or by an individual access from any machine connected to the Internet.

### **Article 12 – Legal and regulatory provisions**

The user shall undertake to respect the effective legal and regulatory provisions, particularly:

The ones related to literary and artistic property present, in particular, into the Intellectual Property Code. Downloading of protected work software or electronic information resources without authorisation from entitled persons shall engage the sole responsibility of user. The Administrator shall reserve the chance to erase from information system any trace of these software and work.

The ones related to Informatics, files and freedoms (law of January 6, 1978).

The ones related to protection of private life and right of the image to others.

Otherwise, the user shall declare to submit to specific rules of use of some resources provided by University and for which he could be informed on the existence of restrictive contractual conditions that link University with third parties, dealing particularly with the use of protected works or electronic information resources.

Besides, in accordance with the principle of commercial neutrality applicable to Universities, the user shall refrain from advertising for commercial products or services, within the framework of information dissemination about spaces provided on University campus.

In accordance with the principle of political and religious neutrality applicable to Universities, the user shall refrain from taking a stance on general political topics that do not treat directly on University's goals and from communicating religious proselytism.

Spaces for the expression of trade unions and societies could be created in order to allow the free expression of opinions from students and staff in accordance with provisions of the Education Code.

The user shall refrain from producing racist, pornographic, paedophile, insulting or defamatory contents or that incites to use prohibited substances, to commit crimes or offences, that incites to suicide or likely to generally cause damage to the image of academic community.

The user shall also refrain from consulting or downloading documents from illicit websites, particularly paedophile or xenophobic websites.

Should the manager states a failure from user to these obligations, it shall lead to his immediate exclusion of services provided.

Moreover, the University shall denounce any penal offence to judicial authorities, without prejudice to the application of internal sanction from University or French National Education.

### **Article 13 – Contractual obligations of user**

The user shall be allowed to visit some websites for private purposes on condition that this navigation do not hinder the access to other users and do not disturb the good operation of information system because in particular, of the overload of downloaded files.

### **Article 14 – Obligations proper to University staff**

Visiting websites for private purposes shall be tolerated to the extent that this navigation do not hinder the professional access and do not disturb significantly the good operation of user work.

### **Article 15 – Intranet**

Intranet shall work under informatics responsibility of the manager and under editorial responsibility of Assignment and Communication manager.

No user may introduce an element in the website or modify elements produced by University without the authorisation of the manager and the Assignment and Communication manager. The users could formulate any suggestion to these latter regarding content or functioning of Intranet.

Persons would be informed, before dissemination of personal data concerning them such as professional addresses or pictures. They could ask manager to have an access to these nominative data and ask that they be rectified.

### **Article 16 - Creation of personal pages**

The provision of pages shall operate according to a procedure of written request to the manager. This request shall comprise the names, first names, address, and user profession and shall specify the purpose of his request. The manager shall have the right to reject any unclear request or that do not correspond to the goals of University.

Besides, the user shall undertake to respect provisions of the present charter and, particularly its article 9, so be attentive not to establish a link with illicit websites or of which content could be incompatible with the goals of University.

The user shall be informed that he has to provide on his pages only copyright free data for intellectual property and not subject to a protection regarding rules or conventions or because of personal character of data provided.

The user shall engage his sole responsibility for failure to his obligations.

Otherwise, it shall be reminded that University staff have, within the framework of their functions, a general obligation of reservation and protection of personal and confidential data of which they could be aware.

The user shall be informed that he has to ensure data protection of which he has a right regarding intellectual property, particularly by informing other users of the non-transferable character of disseminated content.

The University could not be subject to proceedings and reclamations because of the copy and dissemination by a third party of the contents of personal pages disseminated from users.

## **Article 17 – Participation to discussion forums and services**

The user shall have to use fairly these services by prohibiting the utilisation of a pseudonym.

The user could not engage University to take a statement or disseminate illicit information on these services.

The manager shall have the right to delete any litigious message, without prior information to user.

## **TITLE III – UTILISATION OF ELECTRONIC MESSAGING SERVICE**

### **Article 18 – E-mail address**

Each user shall have an electronic messaging composed of his name and first name. In case of homonymy, the manager will set the attribution rules. The utilisation of a pseudonym or the use of a false name is expressly prohibited, except authorisation of manager who shall ensure the legitimacy of this utilisation.

### **Article 19 – Messaging utilisation**

The private use of messaging (sending and receiving messages) shall disturb as low as possible the normal traffic of professional messages, regarding volume and size of the messages exchanged and format of attached documents.

The manager may limit the format, type and size of electronic messages, including attached documents, sent particularly by memorandum. The non-compliant messages to these limitations or messages containing virus will not be distributed.

Electronic messages will be stocked on server only for a short period defined by the manager but that cannot exceed six months. Beyond this date, messages will be deleted except a written request from user approved by the manager. The University shall not guarantee messaging service will be exempt of any interruption, lateness, security incident or error.

The University shall not guarantee the results that can be obtained through this service, nor the accuracy or reliability of information acquired through its intermediary.

The user shall be informed that University do not operate any surveillance or editorial control on sent and received messages. Actually, the University could not be held as responsible for these contents.

### **Article 20 – Service messages**

Although its extreme easy to use, a special attention must be paid to their writing and dissemination. The electronic message is a written document that can engage the University; it can be recognised as the beginning of evidence to establish a legal fact or act. The hierarchical and signature delegation rules shall be absolutely respected. No electronic message shall be sent to a third party of the services without authorisation of the authority entitled to take a decision.

For that purpose, a nominative electronic messaging by staff will be opened. The access to this messaging is strictly personal. Simultaneously a functional alias will be attributed by service. Only the number of this alias will be announced in posts and annual reports about services.

The users of this alias shall be informed that the contents driven by messaging can be subject to a control from the head of service or informatics services within the framework of their goal to secure network.

Otherwise, the risk of intercepting electronic messages shall require limiting the use of electronic messaging to an external destination of information system to information with non-disclosure, non-strategic and non-sensitive character except encryption ensured in agreement with the manager according to the effective rules.

## **Article 21 – Provisions proper to University staff**

The University shall recognise in accordance with the provisions of Labour Code, that an employee have a right of respect regarding his private life, even during the time of service and on workplace; this one shall include the confidentiality of his correspondences or personal contents.

The user shall bear the full responsibility of personal messages transferred through this messaging. Any illicit or abusive use may lead to the immediate removal of the access to personal messaging service.

Moreover, the user will endeavour to keep on his workstation the possible private correspondences that he could be led to keep in a specific file with his name and the mention “private correspondence”.

## **TITLE IV – SANCTIONS**

### **Article 22 – Sanctions applicable to students**

Besides penal sanctions contained in penal code, students shall incur disciplinary sanctions in case of non-respect of provisions of the present convention.

These sanctions shall be decided by the President after studying the dossier by disciplinary section of University planned in article L.712-4 of Education Code.

The right of access can be definitely withdrawn if a failure is duly noticed by the disciplinary section.

The incurred sanctions shall be set by decree n°92-657 of July 13, 1992 modified that establishes the disciplinary procedure in Public Institutions with scientific, cultural and professional character (EPSCP).

### **Article 23 – Sanctions applicable to staff**

Besides penal sanctions contained in penal code, teachers and research teachers shall incur disciplinary sanctions in case of non-respect of provisions of the present convention. These sanctions shall be decided by the disciplinary section of University planned in article L.712-4 of Education Code.

The incurred sanctions shall be set by decree n°92-657 of July 13, 1992 modified that establishes the disciplinary procedure in EPSCP.

The incurred sanctions by other staff are determined according each regulatory or statutory provision concerning them.

## **TITLE V – FORMALITIES**

### **Article 24 – Consultation with the authorities of University**

Before implementing the present charter, have been consulted:

- The Studies and University Life Council on provisions related to student life,
- The Scientific Council regarding its scientific skills,
- The Institution Joint Committee on provisions related to staff,
- CARI regarding all the provisions.

Subsequent proposals of modification will be brought before these authorities as they regard themselves before adoption by the board of directors of University.

### **Article 25 – Display and formalities**



The present charter will be displayed upon its adoption by the board of directors and will be accessible on the Internet and Intranet of University. Some extracts of this charter will be disseminated to students and staff.