Charter governing the rights and obligations of students in relation to the information systems within HEC PARIS

Scope

By application of Article 1 of the Rules of Procedure, this charter applies:

to any person following a program, irrespective of where that person may be (lecture room, documentation room, community areas, etc.) or within the framework of outside activities related to the courses or programs (seminars, in-company periods, overseas stays, trips, visits, sports activities, etc.).

Information systems concerned

The charter applies to the following categories of systems:

- Any and all teaching applications
- Computer tools
- The computer security or protection systems implemented in the school

Access conditions

Each student is given identifiers after signing the “responsibility commitment form” provided for under the Rules of Procedure.

The identifiers provide access to rights as defined according to the schooling of each student. Such rights are granted solely for the duration of the program in the school.

The identifiers are strictly personal. Under no circumstances are they to be given to any third party, including another student. Each student is therefore responsible for any actions undertaken with the use of his or her identifiers.

Conditions of use

Access to the information systems is strictly limited to the following activities:

- educational activities;
- club activities (after approval from the Management of the school).

Any use for projects failing to fall explicitly within the scope of activity of the school is strictly prohibited without the prior written approval of the Dean.

This is not in any way a personal or private space. In particular, it is prohibited to use the information systems to undertake any work, either for money or free of charge, for any person or entity outside of the school.

When using the computer rooms, students must:

1. Be able to prove their identity via their badge.
2. Refrain from eating.
3. Not bring in any travel bags.

The owner of any personal computer is entirely responsible for any connection thereof to any of the school’s networks and shall take all the customary precautions (antivirus, saving/restoring his/her own data).

Any request for intervention entails a release of correspondence.

For groupware purposes, part of the IT environment at HEC is hosted on Google; consequently, the data privacy rules and terms in use are those determined by Google and are identical for all parties hosted by this provider. Please see the rules at:
http://www.google.com/apps/intl/en/terms/user_terms.html

The HEC Paris IT network is connected via the RENATER network (Réseau National de Télécommunications pour la Technologie, Enseignement et la Recherche), so all users of the HEC Pars IT network must agree to and respect the terms of the RENATER charter, which is available for reference at www.renater.fr.

Observance of property rights and licenses

It is prohibited to make any copies of the software made available and to make any use thereof which fails to comply with the requirements of the authors or the company making the said software available to the school.

Any installation on a self-service or lecture room workstation is automatically erased when that workstation is rebooted. Furthermore, users are authorized to download subject to due observance of the laws on intellectual, literary and artistic property. Reproduction of commercial software and generally speaking of any literary, artistic or musical creation, for any use whatsoever, is strictly prohibited and constitutes an infringement liable to prosecution.

Responsibility for content

Students are responsible for everything they write or put on line. They are solely responsible for any and all removable media (CR Rom, memory stick, removable hard disk, etc.) belonging to them. Use of the graphic charter of the Web site or of the logos of HEC Paris is subject to prior agreement from the Management of the school.

Students undertake:

1. not to broadcast email or publish any content of which they are not the author or for which they do not have written permission from the author and not to transfer outside any messages distributed on the networks of HEC Paris of a confidential nature or contrary to the rules of the IT charter.
2. not to make any use of the personal data and teaching content to which he/she has access other than for his/her own program.
3. to use the electronic messaging system as a specific tool for communication between people and not as a tool of general information.
4. not to harass other users with unwanted messages or by posting/disseminating illegal information (injurious, pornographic, defamatory, racist, etc.).
5. to refrain, by the nature of his/her messages and/or acts, from impairing the image or the interests of the school or of the CCI Paris Ile de France. Any use of the names and logo of the school or of the CCI Paris Ile de France is subject to prior written permission from the Management of the school.

Contributions to social media

Students are expected to use reasonable language towards their school, its teachers and the CCI Paris Ile de France.

It is prohibited to disclose information of which students have knowledge by their belonging to the school.

It is also prohibited to disclose the details of the persons working in the school.

Observance of security of the information systems

The CCI Paris Ile de France has implemented security measures to guarantee its information systems and the personal data put on line.

Students undertake to observe these security measures and in particular not to attempt in any way whatsoever to impair the integrity of the computer systems of the school both in classes and in self-service or in residence and not to undertake any action likely to adversely affect their smooth operation. In particular, students undertake not to modify the work environment of other users and not to attempt to obtain access to user spaces other than those allocated to them.

Students shall refrain:

1. from introducing data or programs likely to disrupt the smooth operation of the computer systems of the school.
2. from trying to intercept communications between users.

Use of the computer systems

Each student **undertakes to:**

- have an up-to-date antivirus and to apply the patches of the editors concerning the security of the operating system running on his/her computer
- to take up only the quantity of disk space that is strictly necessary and to make optimal use of the file compression resources available.
- to run processing which involves extensive use of the computer resources (printing of large documents, large scale calculations, intensive use of the network, etc.) at times which penalize other users the least.
- to assume responsibility for the rights granted to other users on his/her workstation or in spaces made available by HEC Paris.
- Respect the general clauses of use of the external platforms and be responsible for his/her commitment towards the providers to HEC (Jobteaser, Google.)

Not to:

- use any account (username) other than that to which he/she has a right of access,
- perform any maneuver aimed at misleading other users as to his/her identity,
- attempt to capture or decipher the password of other users,
- attempt to restrict or forbid access to the computer systems of authorized users.
- leave a workstation with the session still open,
- develop self-duplicating programs or programs which attach themselves to other programs (computer viruses).

If a student notices a malfunction or an anomaly in the resource used, he/she must report it to the professor in charge or to the computer assistant indicating the workstation concerned and the nature of the anomaly.

Use of these resources is reserved for educational activities as defined by the school. They are not in any way a personal or private space. Users must be prepared at any time to justify the condition and the content thereof.

It is prohibited to physically move the hardware and to make any modification to the connections of the hardware to the electrical, telephone and computer networks without having previously obtained the written permission of the IT Department.

Each student undertakes not to make any operation which may result in:

- interrupting the normal operation of the network or of any one of the systems connected to the network,
- giving access to the data of another user of the network without his/her permission,
- alteration or destruction of the data of any one of the systems connected to the network.

Role of the administrators and verifications of use

The systems/network/SGDB/WEB administrators are the people who manage the machines connected to the HEC Paris network and the servers on which the various services available to users are installed (Internet, management applications, teaching services, services for research and documentation).

In that capacity:

- they are in charge of the quality of the service provided to users within the limits of the means allocated. They are entitled to undertake any action required for the smooth operation of the computer resources of HEC Paris;
- insofar as possible, they are required to inform the users of any necessary intervention likely to disrupt or interrupt the customary use of the computer resources;
- they have the possibility of consulting, after the event, the data published in the public and private spaces, such as, for example, a Website, a cooperative work space or forum made available for teaching purposes and to report any behavior contrary to the present charter;
- they are obliged to preserve and observe the confidentiality of any such private information of which they may gain knowledge within the framework of their activity.

All the actions undertaken from the network and workstations are traced and enable identification of their author. This type of tracing is employed solely for technical use. Within the framework of any legal proceedings, however, the files may be made available to the courts.

The Computer Department is responsible for guaranteeing the proper use of the information systems and can in that respect:

1. obtain access to messages sent or received by a student;
2. analyze the documents put on the network or on a workstation.

It may take any and all conservative measures (shutting down the systems, confiscating rights of access, locking files, etc.) to prevent any overload of the resources, freeze a status due to problems related to the security of the systems. The latter keep the information concerning, for example, the messaging system (sender, addressee(s), dates but also times of connection) or access to Websites. This type of tracing is employed solely for technical use. Within the framework of any legal proceedings, however, these files may be made available to the courts.

The acts committed may result in the suspension or cancellation of the access rights of a student, for fifteen days or permanently.

Applicable sanctions

Any student failing to observe the provisions of the present charter is liable to sanctions as defined in Chapter V of the Rules of Procedure.