Charter for the use of digital resources of the University of Geneva

--- Related keywords: IT resource, IT security, IT systems, information and communication technology system

This Charter defines the rights and obligations of users of digital resources of UNIGE.

We are all responsible for the smooth functioning of the IT system and for keeping data safe!

This DIRECTIVE is an official translation of the DIRECTIVE 0296 « Charte d'usage des ressources numériques de l'Université de Genève » published on March the 16th 2017 in the University of Geneva MEMENTO. In the event of inconsistency or discrepancy between the English and the French version of the Directive, the French version shall prevail.

Summary

1. USER STATUS AND RIGHTS
2. PROPER USE OF DIGITAL RESOURCES
3. PRUDENT MANAGEMENT OF INFORMATION AND DATA
4. RESPONSIBLE USE OF "BRING YOUR OWN DEVICE (BYOD)" EQUIPMENT
5. PROFESSIONAL SYSTEMS MANAGEMENT
6. SURVEILLANCE MEASURES
7. POSSIBILITY OF SANCTIONS
8. ACCEPTANCE OF THE CHARTER

1. USER STATUS AND RIGHTS

Each authorized user of the IT system has the right:

- to the digital resources required for the successful carrying out of his or her University activities, subject to the limitations of UNIGE;
- to access to digital resources appropriate for his or her user profile;
- to information related to digital services made available by UNIGE;
- to protection of his or her personal data that complies with relevant federal and cantonal requirements.

Users are understood, essentially, to be members of the instructional faculty, members of the administrative and technical personnel, UNIGE students, and external persons called upon to collaborate with UNIGE in the framework of research, instruction, or the provision of services.
2. PROPER USE OF DIGITAL RESOURCES

- Digital resources are understood to be digital equipment, services, and data, including computers, the digital network (including access to the Internet and to the local wired and Wi-Fi network), servers, printers, telephones, databases, software, and online services.

- Only professional use of these resources, directly related to academic activities, appropriate for the accomplishment of assigned tasks or the studies of the user, is authorized. Their utilization for personal purposes is only tolerated if it is minimal in time and frequency, if it only accounts for minimal resource use, if it does not compromise or interfere with professional activities or activities of the Institution, if it is not related to private for-profit activities, and if it is neither illicit nor contrary to civility or decency.

- Each user shall receive a nominative credential. He or she is responsible for the usage that he or she makes of digital resources, and for activities that occur using his or her credential, and he or she undertakes to refrain from activities that could harm the UNIGE IT system. In no case may he or she usurp the identity of another, or act anonymously.

- Information disseminated, in particular via the Internet or email messages, must conform to law, to common decency, to dignity, and to the reputation of UNIGE and its members. Statements that are defamatory, calumnious, injurious, racist, sexist, violent, or pornographic, are specifically prohibited.

- The sending of email messages to large numbers of employees or students is based on the mechanism of mailing lists. Any other means of dissemination (specifically including copying addresses from the directory) is considered spamming, and is prohibited.

- The user may only install and/or use software that is not subject to copyright or that is covered by a license that authorizes him or her to do so, whether the software is provided by UNIGE or acquired by the user.

- The use of Cloud storage, processing, exchange, or synchronization services for sensitive UNIGE data, notably data pertaining to persons and certain research data, is prohibited in the absence of legal guarantees sufficient for the protection of the data (confidentiality, copyright, patentability) and based on the application of laws and regulations governing personal data. Users are encouraged to instead use equivalent services provided by UNIGE or SWITCH (Swiss Cloud services reserved for the University community). These are available through the Catalog of digital services.

- Users shall take good care of devices assigned to them or made freely available to them in computing labs, libraries, and public spaces. They shall use them in a manner respectful of the environment. It is prohibited to disconnect devices freely available for use, and these devices must be used in a manner respectful of the spaces and other users present.
3. PRUDENT MANAGEMENT OF INFORMATION AND DATA

- A user charged with managing a file containing personal data must ensure that such a file is managed in conformity with the Directive detailing the implementation of LIPAD at UNIGE.
- The user shall respect provisions related to intellectual property in the framework of his or her academic or administrative activities, including when he or she copies, uses, modifies, disseminates, or destroys documents, data, or research results, or when using software. It is prohibited to disseminate information that is not explicitly public without the prior consent of its owner.
- Use of peer-to-peer file-exchange software to download or share copyright-protected materials or software is prohibited.
- Clear guidelines for the use of video surveillance systems are set down in “Installation and use of a video surveillance system”, available in the Memento.
- Upon departure from UNIGE, and unless expressly agreed otherwise, the user must ensure that non-public UNIGE data and documents, and software provided by UNIGE and under license that he or she used in the framework of his or her activities, are returned to UNIGE.

4. RESPONSIBLE USE OF “BRING YOUR OWN DEVICE (BYOD)” EQUIPMENT

- Students and employees are authorized to use BYOD devices in the framework of their studies or the accomplishment of assigned tasks.
- Users who connect to UNIGE digital resources with BYOD devices are responsible for their proper functioning and safety (systems up to date, security patches installed, anti-virus activated, etc.).
- UNIGE only provides limited IT support for BYOD devices.
- UNIGE can require a user to install software on their BYOD device that makes it possible to protect it and verify its safety, to ensure a secure connection to the network, and to protect data or software utilized in the framework of the user’s institutional activities.

5. PROFESSIONAL SYSTEMS MANAGEMENT

- Users having been authorized, in the framework of their activities, to install and configure active systems on the network (Windows/Mac/Unix, web servers, NAS/storage components, etc.) must comply with the general security regulations that ensure the proper functioning of the IT system.
6. SURVEILLANCE MEASURES

- In accordance with its responsibilities and in compliance with legal provisions, UNIGE puts in place digital surveillance measures in order to ensure the security, access, and proper functioning of digital resources. To that end, sample-based controls are also conducted in order to ensure that the principles in the present Charter are respected.

- Within the framework of legal constraints, the use of digital resources is recorded (IP addresses and URLs visited,...) and these records may be viewed by duly authorized administrative or judicial authorities. A user’s access to resources may be exceptionally blocked, as stipulated in the applicable procedures.

7. POSSIBILITY OF SANCTIONS

- Failure to abide by the principles in the present Charter may result in removal of access to digital resources, and even to disciplinary sanctions.

- Provision is made for recourse to civil or criminal law.

8. ACCEPTANCE OF THE CHARTER

- Accessing the UNIGE digital network and using UNIGE digital resources implicitly requires each user to comply with the present Charter, the Security policy for the IT system, and its annexes.

1 Peer-to-peer (P2P) is a technology that facilitates the sharing of resources between Internet users, in particular by allowing the sharing of files stored on the hard drive of their devices.

2 BYOD is an acronym for “Bring Your Own Device”. It refers to the practice of using one’s own devices (tablet, computer, telephone) in the framework of one’s work. At UNIGE, this concerns all devices not allocated by UNIGE, but purchased and managed by the user or another institution.