Regulations relating to the use of ICT facilities at Utrecht University

Article 1 Definitions

In these regulations the following definitions are being used:

a. ICT facilities:
   All hardware, software and network facilities provided by Utrecht University (hereinafter: UU), as well as all electronic data and speech traffic facilities;
b. Administrator:
   The UU department responsible for the operational availability of the ICT facilities;
c. User:
   Anyone who is employed by or is studying at UU and anyone who on any other grounds has been authorised to use the ICT facilities.

Article 2 Authorised use

The University provides computer facilities and access to its computer networks only for purposes directly connected with the work of the University and with the academic activities of its students. Login codes are personal. In case of an employee's absence due to illness, it may be necessary that the information behind a login code, such as e-mail, is consulted by either colleagues or the supervisor. Agreements on this will be made between the management and the employee in accordance with the current absence protocol. For further information, see http://www.uu.nl/NL/Informatie/medewerkers/arbeidsvoorwaarden/Documents/Verzuimprotocol.pdf (in Dutch).
Use of ICT facilities for private purposes is permitted as long as this does not disrupt the daily activities of user or others.

Article 3 Unauthorised use

1. Any form of use of ICT facilities that is in breach of legislation or the stipulations of these Regulations, specifically usage that imperils the administration, maintenance, security, integrity, quality or continuity of services provided by UU, that disturbs UU processes, or that financially damages or defames UU, ICT users or third parties, is not permitted.
2. In addition, it is not permitted:
   a) To install additional hardware or software onto ICT facilities or to start these up, unless this is necessary in order to perform their duties or attend academic activities and this is part of the ICT arrangements confirmed by the administrator involved;
   b) To use another person's name in order to make use of, turn off or by-pass ICT facilities or security measures, nor to make personal login codes known to others;
   c) To make use of ICT facilities in order to gain unauthorised access to non-public or secured sources of information or to provide information to others through such sources;
   d) To make use of ICT facilities that have been made available within the university's public areas and grounds, in order to gain access to sources of information that provide pornographic, racist, discriminating or offensive material, unless this is demonstrably essential to the research by or education of user;
   e) Without authorisation, to change, delete or add to information that has been accessed through the use of ICT facilities;
   f) To use ICT facilities in a way which causes a nuisance to other users or third parties;
   g) To use ICT facilities for private purposes with a commercial character;
   h) To use ICT facilities for sending or forwarding threatening, offensive, sexually oriented, racist or discriminating messages;
   i) To disseminate with the aid of ICT facilities any material protected by copyright without prior permission from the copyright owner. It is only permitted to download software, films, music etc. when this is essential for staff or students to perform their duties or attend academic activities, with due regard to copyright and to the licensing contracts agreed upon by UU.

Article 4 Reporting

UU has set up an email address (abuse@uu.nl) for users to report any instances of unauthorised use of ICT facilities. All reports will be treated confidentially; however, reports will not be handled anonymously.

Article 5 Registration and checks

UU does not accept any forms of unauthorised use of the ICT facilities provided by UU. To safeguard the use of ICT facilities, a system of registration and checks has been set up. As a result, the use of ICT facilities is registered and consequently will be monitored by random checks at regular intervals. Specific checks may be carried out if UU has sufficient grounds to do so. Checks are either carried out by specially appointed staff or take place electronically. The stipulations of the Personal Data Protection Act apply to the registration of ICT use. Based on statutory provisions, UU may be obliged to provide third parties with (partial) information from this registration.

Article 6 Sanctions

In the event of observed forms of unauthorised use, UU will take action against the abuser. The seriousness, duration and frequency of the violation, its consequences, and the level of material and immaterial damage will be taken into account when setting the terms of the sanction. Insofar as UU employees are concerned, the university regulations regarding Order and Disciplinary Measures (based on the Collective Labour Agreement for the Dutch Universities) apply.
If so desired or if deemed necessary, UU is entitled to call in investigative authorities. In addition to this, UU may decide to take appropriate legal action.

Article 7 Implementation

These Regulations take effect from 1 March 2008 and shall replace all previous User Regulations.

These terms will also be available in Dutch. In case of any dispute on the contents or meaning, the Dutch text shall prevail.

Explanory Notes

General

Within UU, extensive use is made of ICT facilities. Nearly all university processes depend on ICT. In order to safeguard the availability, integrity and confidentiality of information and information services, the Executive Board has decided on a University Information Security Policy. This policy has been laid down in the 'Policy and Basic Regulations regarding Information Security at Utrecht University' policy document. The objective of this policy is to set up and monitor a balanced system of security measures aimed at decreasing the number of risks. The information security policy is being implemented through a combination of regulatory procedures and technical measures.

Technical measures alone are not sufficient to safeguard the functionality of ICT facilities. Unauthorised use of facilities by single users may result in a lot of trouble or damage, thereby duping other users. To prevent this, rules have been laid down for the responsible use of ICT facilities provided by Utrecht University. They are included in these User Regulations. Anyone making use of ICT facilities must abide by these User Regulations. ICT facilities include, among other things: applications (such as E-mail and Internet), computers, telephone and the university network.

These Regulations apply in the first instance to staff and students of Utrecht University who make use of ICT facilities within the buildings and grounds of the university. They also apply to the use of university facilities (such as an E-mail address or E-mail account) outside the university. In addition, the Regulations apply to all other persons making use of the ICT facilities of Utrecht University, such as seconded staff, visiting staff, trainees, temporary staff etc.

The core of the Regulations is laid down in Articles 2 and 3, listing a number of general rules regarding the authorised and unauthorised use of ICT facilities. By these User Regulations, Utrecht University aims to prevent any obstruction or offence as a result of the use of these facilities.
The UU has set up an e-mail address to report any unauthorised use to. In addition there is a system of registration and checks. In the event of unauthorised use of ICT facilities, appropriate actions will be taken against the offender.
The University attaches great value to the ICT users' respect for general social merits. To safeguard this aspect of electronic communication, a model-netiquette has been laid down in addition to the User Regulations. The Netiquette includes 11 rules of thumb referring to correct ICT behaviour.

Specific articles of the User Regulations

Article 2

In principle, ICT facilities are available for education, research and the UU's general business operations. ICT facilities, therefore, are primarily intended for the work of the University and the academic activities of its students.
Private use is permitted as long as this does not disrupt the daily activities of the user. The UU staff bear responsibility for this, to the final judgement of the manager. Furthermore, private use of ICT facilities shall not disturb others. The downloading or forwarding of exceptionally large files, for instance, may place an unacceptable burden on parts of the university network.

Article 3

The use of ICT facilities includes certain risks which induce the laying down of user regulations. These risks include:

- Security risks, such as damage to the ICT infrastructure through viruses and intrusion by computer criminality;
- Legal risks, such as the breach of intellectual property through illegal downloads, the downloading of child pornography, and abuse or discrimination via electronic methods;
- Ethical risks, such as the discrediting of the good reputation of UU and others;
- Costs: the improper use of communication media may involve unnecessary costs. Added to this is the realistic risk of damage claims by victims;
- The risk of systems crashing or the overloading of the ICT infrastructure: unwanted applications may seriously disturb the regular performance of various systems within UU.

In Article 3, consequently, a general list of unauthorised use is given including usage which:

a) Breaches legislation. Use of ICT facilities has to operate within the law. Therefore, illegal copying of software or the use of illegally copied software is not permitted;
b) Imperils the administration, maintenance, security, integrity, quality and continuity of ICT services provided by UU. Integrity may be threatened, for instance, by the unauthorised changing of data in a system (e.g. student marks in OSIRIS). Continuity may be in danger as a result of a web server or a website being bombarded by data (i.e. a denial-of-service attack);
c) Disturbs the UU business operations. The primary processes and the UU business operations must not be threatened or disturbed. This may, however, occur through the sending of exceptionally large numbers of e-mail which can cause an overload, or even a fuse of the university computer systems;
d) Causes financial damage to or defames UU, users or third parties. It is not permitted to carry out activities which may cause such damage.

In addition to the general prohibitory stipulation, Article 3 lists all forms of unauthorised use including the following examples. It is, for instance, not permitted to use ICT facilities in another person's name. It is also not permitted to intercept or make use of another person's login codes. Conversely, it is also forbidden to share one's personal login codes with others. Staff, users and students are not permitted to use ICT facilities for private purposes of a commercial character because software and Internet connection licences entered into by UU do not allow for commercial use. UU does, however, promote entrepreneurship among its students. Education pays attention to the starting of businesses and the Centre for Entrepreneurship and Innovation provides support and advice to starting entrepreneurs, researchers and students.

Article 5

Utrecht University will monitor the observance of these Regulations by random rather than continuous checks.

The policy regarding checks of the use of UU ICT facilities is as follows:

- In principle, checks are carried out at the level of totalised data which are not to be traced to individual persons. If there is reason to suspect certain individuals of non-compliance with the Regulations, specific checks may be carried out during a set (short) period of time;
- In principle, checks are restricted to traffic data regarding the use of E-mail and Internet. Based on sufficient grounds only, content checks may be carried out;
- Staff who demonstrably disregard the Regulations will be called to account by their managers as soon as possible;
- In principle, e-mail messages from or to staff in confidential positions are excluded from checks. This does not apply to e-mail traffic security checks.

If there is reason to suspect individuals or a group of individuals of non-compliance with the Regulations, specific checks may be carried out during a set period of time. As much as possible checks will be tailor-made and of as limited a scope as possible, in accordance with privacy legislation.

It is not required to report the registration of the use of ICT facilities to the Data Protection Board as this is covered by the exemption scheme.

Article 6

In case of non-compliance with the User Regulations, the Executive Board as well as the mandatory is entitled to impose further sanctions. Sanctions applied will be in correct proportion to the proved abuse.

There is no list of sanctions for each offence. It is up to the Executive Board or the mandatory to decide on:

a. The seriousness of the offence;
b. The duration and the frequency of the offence or offences;
c. The consequences of the offence and the scope of any material or immaterial damage.

Based on these conclusions the Executive Board or the mandatory will decide on the terms of the sanction. Sanctions may include:

- Temporary or permanent restriction of access to specific ICT or telephone facilities;
- A temporary or permanent ban on the use of specific facilities;
- Recovery of the costs ensuing from the offence;
- In case of staff: termination of employment, or in case of other users: termination of the grounds on which user had access to the facilities.

Other measures may apply as long as these are deemed suitable. For instance, students sending bulk mail from their mailbox unrelated to any study assignments will be warned to stop this

immediately. If they do not act upon this warning or even repeat this action their mailbox will be blocked for a set period of time. The students' access to the electronic learning environment will not be restricted, so as not to impede their studies.

Measures against staff are based on Article 6, paragraphs 12 and 15, of the Collective Labour Agreement for the Dutch Universities and the University regulations regarding Order and Disciplinary Measures (see appendix). Employees may lodge a complaint with the Executive Board against specific decisions or appeal to the Court of Law.
Measures against students are based on Article 7.57h of the Higher Education and Research Act (see appendix). This Act restricts any refusal of access to buildings or facilities to a period of time not exceeding one year. Students may lodge a complaint with the Executive Board against specific decisions or appeal to the Higher Education Appeals Tribunal.
Measures against other users are not based on specific legislation. If no sanctions are laid down in the agreement which is the basis of the user's access to the university facilities, the right to act against abuse follows from the university's property rights. In this case no complaints or appeals can be filed, unless specific stipulations are laid down in these Regulations.

Appendix: relevant regulations and stipulations