Code of Conduct on ICT and Internet Use

by Students

University of Twente

2011

TABLE OF CONTENTS

Introduction

This Code of Conduct shows the way in which the University of Twente deals with ICT and internet use. The code arranges the responsible use of ICT facilities and the internet and the way in which the use is monitored. The ambition is to create the right balance between a responsible and safe ICT and internet use and the privacy of the student-user.

Because a separate Code of Conduct for ICT and Internet Use has been formulated for users other than students, this code does not apply to these users.

In formulating this code of conduct, we have sought to comply with the Personal Data Protection Act (the *WBP*). This Act is applicable if the processing of personal data is involved. Processing of data concerns the entire process from collection up to the destruction of data. Data pertaining to the email and internet use can generally be qualified as personal data for reason that these data can be traced to natural persons.

1. Definitions

In this scheme the following is understood to mean:

a. **Manager**: the natural person charged with the management of the faculty (dean), the research institute (scientific director) or a service department (director).

b. **CERT-UT**: the Computer Emergency Response Team of the University of Twente, established in order to tackle and where possible to prevent, under the responsibility of the ICTS director, computer security problems within the University of Twente.

c. **Executive Board**: Executive Board of the University of Twente.

d. **Director ICTS**: the director of the ICT-Service Centre of the University of Twente.

e. **Student-user**: each student as referred to under l. or resident of a student campus accommodation that makes use of the ICT facilities that are made available by the University of Twente, including a student who manifests himself with an ICT workstation and an identity from the University of Twente (IP number of the University of Twente or a domain name under the principal domain UTWENTE.NL).

f. **Code of Conduct**: the Code of Conduct on ICT and Internet Use as laid down in this document.

g. **ICT and internet use**: any use via the UTnet, SURFnet or internet of ICT facilities offered by the University of Twente, including email facilities.

h. **ICT officer**: each employee of the University of Twente having a position with the ICT Service Centre, the director ICTS, as well as any other persons performing ICT activities under the responsibility of the University of Twente.

i. **ICT workstation**: a computer (PC, Laptop, PDA, and suchlike) that is owned by the University and which is used by the student for ICT and internet use.

j. **Network equipment**: all equipment that the University applies for an efficiently functioning UTnet (routers, switches, DNS servers, et cetera).

k. **Personal data**: all data that can provide information about an identifiable natural person.

l. **Student**: every person who is enrolled as a student at the University of Twente or who follows education at the University of Twente.

m. **SURFnet:** the national network infrastructure managed by SURFnet BV, with which the local networks of the higher education institutions and research are mutually connected and to which the UTnet is linked.

n. **SURFnet BV:** the company ("BV") under Stichting SURF that manages the SURFnet.

o. **Access configuration**: settings of ICT stations, servers and network equipment owned by the University for the identification of the system on and network traffic over the network.

p. **Access key**: a combination of the student user name and password or other authentication facility that authorises the student-user to use ICT facilities of the University of Twente.

q. **University**: University of Twente.

r. **UTnet**: the intranet of the University of Twente, both wired and wireless, that connects all computer systems within the University with one another, including home stations which are directly connected, and which is linked to SURFnet and internet.

s. **Traffic data**: data over network use, access use and computer use such as account name, source, sender, addressee, destination, date, time and size.

t. **Wbp**: Personal Data Protection Act.

u. **Employee**: anyone having an employment contract with the University of Twente or anyone who works at the University of Twente on a different basis.

2. Scope

2.1. This Code of Conduct applies to each student as referred to under 1.e. and 1.l. of this scheme who makes use of the ICT facilities offered by the University, including email facilities.

3. ICT and internet use general

3.1. The purpose of this Code of Conduct is to provide clarity to student-users about the context in which ICT and internet use is to take place at the University and what measures can be taken if this Code of Conduct is violated.

3.2. In using ICT and the internet, the student-user will abstain from any actions that may harm the reputation of the University or which are unlawful or punishable.

3.3. The access key granted by the University to the student-user is strictly personal and remains the property of the University. It is not allowed to provide the access key to third persons, unless in the opinion of the manager this is necessary for an adequate participation in the educational activities. The person to whom the access key has been provided, is obliged to do or omit anything that can reasonably be expected from him/her in order to prevent abuse of the access key provided. The person who issues the access key is obliged to point out this code of conduct to the receiver.

3.4. A student-user may grant a technical authorisation to a third person to obtain access to his/her email facility (including agenda). The third person will use his/her own access key for this.

3.5. If any security incidents are found or suspected, the student-user must report the incident immediately to the CERT-UT.

3.6. The student-user is not allowed to change the access configuration of the ICT workstations, servers and network equipment owned by the University.

3.7. The student-user is not allowed to disclose any non-public information or services on the UTnet in any way to the outside world without the prior approval of the ICTS director.

3.8. The student-user is not allowed to connect to the UTnet any network equipment (such as routers and switches) that may cause inconvenience. The starting point is that students are to comply with the rules as laid down in the *Acceptable Use Policy Studenten Net Twente* approved by the ICTS director. This document can be obtained via *Studenten Net Twente* and can be viewed via the website of Studenten Net Twente.

3.9. The student-user is not allowed to send or store any threatening, (sexually) intimidating, (child) pornographic or racist or otherwise discriminating email messages or, in using ICT facilities of the UT, to consciously visit internet sites that contain (child) pornographic, racist or otherwise discriminating material, unless this is necessary with regard to the free gathering of information in the context of the study, and approval for this has been given by the manager.

3.10. Under the responsibility of the ICTS director email messages from and to the University are checked for malware (viruses and suchlike) and spam. If necessary, contaminated messages are removed or malware is discarded.

3.11 When using the email box made available by the University, the student-user must use as sender an email address that has been provided to the student-user by the University. The student-user is not allowed to make the email address available as sending address to other persons.

3.12. The student-user is not allowed to read, copy, change or delete email messages intended for other persons unless the addressee has give explicit consent for this.

3.13. The user is not allowed to download excessive amounts of articles from the files of the digital library or to systematically copy substantial parts of the files of databases in the digital library. The copied article are for personal use only.

4. Back-ups

4.1. Without a notice to the contrary of ICTS, the student-user may assume that the back-up procedures at the University yield reliable back-ups. If the student-user uses media for data storage for which no standard back-up is made, he/she must see to this himself/herself. If necessary, in consultation with ICTS.

5. ICT and internet use by the student-user

5.1. The student-user is held to make use of the ICT and internet use for his/her study.

5.2. The student-user is allowed to make limited use of the ICT and internet for personal use.

5.3. Students living on the UT Campus and for internet access in their accommodation make use of the UTnet and SURFnet, are not subject to any limitations to the personal use in their accommodation. The other provisions in this Code of Conduct are fully applicable to student-users living on the campus.

5.4. Commercial use of SURFnet is only permitted if in the opinion of the manager this use is related to education and research in UT context.

6. General supervision

6.1. The purpose of general supervision is system and network security and is performed by an ICT officer on the instructions of the ICTS director.

6.2. CERT-UT can check traffic data in the event of a security incident with the sole purpose of finding and removing the cause of the incident or to limit the consequential loss of the incident. In this context CERT-UT may impose temporary restrictions on the student-user in his/her access to certain ICT facilities.

6.3. In principle, traffic data on ICT and internet use are kept for a maximum period of six months. In the event of a directed investigation as referred to in article 8, these data may be kept longer until the necessity to do so no longer exists.

6.4. The ICT officer has an obligation of secrecy with regard to data pertaining to ICT and internet use that are traceable to persons.

7. Directed investigation

7.1. In the event of a suspicion of use in violation of the Code of Conduct, the student-user in question will be address about his/her conduct by the manager as quickly as possible.

7.2. Directed investigation into a person takes place in response to a justified suspicion or the establishment of incorrect use as referred to in the articles 3, 5 and 6 of this Code of Conduct. The main objectives of directed investigation are:
- establishing inappropriate ICT and internet use;
- checking agreements made on (prohibited) use;
- preventing negative publicity about the University as a result of punishable use.

7.3. The directed investigation takes place after a written instructions from the Executive Board to the ICTS director and is conducted by an ICT officer appointed for this. The instruction of the Executive Board will state why the investigation is held and why – in so far as relevant – the student-user will only be informed of the investigation afterwards.

7.4. The Executive Board will be informed in writing about the results of the investigation. If the investigation gives no cause for further measures, the written report will be destroyed.

7.5. Only in the event of compelling reasons will a directed investigation be conducted into the content of emails and files stored. These reasons will be stated in the written instructions of the Executive Board.

7.6. Email messages and files of university council members, faculty council members and members of the programme committee who are in office are not excluded from the general supervision of the system and network security but are excluded from a directed investigation in so far as the emails and files concern their functioning as a member of the participation committee/programme committee.

7.7. The student-user against whom an investigation as referred to in article 7.3 is conducted, will be informed as quickly as possible by the Executive Board about the reason, the execution and the result of the investigation. The student-user will be given the opportunity to give an explanation with regard to the data found. The provision of information to the student-user is postponed if this harms the investigation.

7.8 Illegal software, films and music and emails and files that concern that which has been mentioned under article 3.9., will be removed on the instructions of the manager. The student-user will be informed about this in advance unless this hinders the investigation.

8. Sanctions

8.1. if the student-user acts in violation of the Code of Conduct, the Executive Board can impose the following sanctions:
a. permanent or temporary restricted access to certain ICT facilities;
b. temporary or definitive ban on using certain ICT facilities;
c. payment of costs arising from the abuse established.

9. Liability

9.1. The University retains the right to hold the student-user liable for damage caused by the student-user as a result of ICT and internet use by the student-user. This also includes compensation claimed from the University by a third party as a result of acts conducted by the student-user in violation of this Code of Conduct.

9.2. The University excludes any liability for damage arising from the use of and the inability to use (part of) the University's ICT facilities.

10. Final provisions

10.1. Two years after its implementation, this Code of Conduct will be evaluated.

10.2. The Wpb is fully applicable.

10.3. This Code of Conduct was adopted by the Executive Board on 30 May 2011 with the approval of the University Council given on 6 April 2011.