Code of Conduct on ICT and Internet Use

University of Twente

2009

TABLE OF CONTENTS

Foreword
1. Definitions
2. Scope
3. ICT and use of the internet general
4. Back-ups
5. ICT and the use of internet by employees
6. General supervision
7. Directed investigation
8. Sanctions
9. Liability
10. Final provisions

Foreword

This Code of Conduct sets out the way in which the University of Twente handles ICT and use of the internet. The Code provides for the sensible use of ICT facilities and the internet and the way in which the use is monitored. The ambition is to achieve a satisfactory balance between a sensible and safe use of ICT and the internet and the privacy of the user.

Because a separate Code of Conduct for the use of ICT and the internet by students will be drawn up, this code is not applicable to students who make use of the ICT and internet facilities of the University of Twente.

In preparing this code of conduct, we have linked up with the Dutch Personal Data Protection Act (WBP). This Act is applicable if processing of personal data is involved. Processing concerns the entire process from collecting to destroying data. Data concerning email and internet use can generally be qualified as personal data because these can be traced to natural persons.

1.Definitions

In this Code of Conduct the following is understood to mean:

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

b. **CERT-UT:**
the Computer Emergency Response Team of the University of Twente, instituted for tackling, and, where possible preventing, computer safety problems within the University of Twente under the responsibility of the director ICTS.

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

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

e. **User**:
anyone – with the exception of the student as referred to under k.– who makes use of the ICT facilities made available by the University of Twente, including anyone who manifests him or herself on the internet using an ICT workplace with an identity of the University of Twente (IP number of the University of Twente or a domain name under the main domain UTWENTE.NL).

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

g. **ICT and use of the Internet**:

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

h. **ICT officer**:
each employee of the University of Twente with a job falling under the ICT Service Centre, the director ICTS, and any other persons who perform activities in the field of ICT under the responsibility of the University of Twente.

i. **ICT worplace**:
a computer (PC, Laptop, PDA, and suchlike) used by the user for ICT and the use of the internet.

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

k. **Student**:
anyone enrolled as a student at the University of Twente or who is doing a study programme at the University of Twente.

l. **SURFnet:**
the BV (private company with limited liability) under Stichting SURF that manages the SURFnet.

m. **SURFnet BV:**
de BV onder Stichting SURF die het SURFnet beheert.

n. **Access configuration**:
set-ups of ICT workplaces, servers and network equipment for identification of the system on and network traffic across the network.

o. **Toegangssleutel**:
een combinatie van gebruikersnaam en wachtwoord of andere authenticatiefaciliteit die de gebruiker autoriseert tot gebruik van ICT-voorzieningen van de Universiteit Twente.

p. **University**:
University of Twente.

q. **UTnet**:
the intranet of the University of Twente, both wired and remote, which connects all computer systems within the University with one another, including directly connected home workstations, which are linked to SURFnet and the internet.

r. **Traffic data**:
data about network, access and computer use, such as account name, source, sender, addressee, destination, date, time and volume.

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

t. **Employee :**
anyone who is employed by the University of Twente or anyone who works with the University of Twente on any other basis.

2. Scope

2.1. This Code of Conduct is applicable to anyone - with the exception of the student as mentioned under k. of the definitions - who makes use of the ICT facilities offered by the University, including email.

3. ICT and use of the internet general

3.1. The purpose of this Code of Conduct is to explain to users the framework within which ICT and the use of internet is to take place within the University, and which measures can be taken in case of activities that are in violation of this Code of Conduct.

3.2. In using ICT and the internet, the user will refrain from activities that may harm the reputation of the University, or which are unlawful or punishable.

3.3. The access key provided by the University to the user is strictly personal and remains the property of the University. It is not allowed to provide the access key to third parties, unless this is necessary for an adequate performance of the activities, and then only after permission of the administrator. The person to whom the access key has been provided is obliged to do or omit all that may reasonable be expected from him/her to avoid misuse of the access key provided.

3.4. A user may himself authorise a third person technically to gain access to his email facility (including agenda). The third person uses his own access key for this.

3.5. In the event of any demonstrable or suspected safety incident, the user must report the incident forthwith to the CERT-UT.

3.6. The user is not allowed to change the access configuration of ICT workplaces, servers and network equipment of the University.

3.7. Without the prior permission of the director ICTS it is not allowed to disclose non-public information or services on the UTnet to the outside world in any way.

3.8. The user is not allowed to connect other network equipment (such as routers and switches) to the UTnet than network equipment for which the director ICTS has given permission.

3.9. In using ICT and the internet, the user may not disrupt or disproportionately burden the ICT infrastructure of the University.

The user is at any rate not allowed to download large numbers of articles from the files of the digital library or to systematically copy substantial parts of the files or databases in the digital library.

3.10. The user is at any rate not allowed to consciously visit internet sites that contain (child) porn, racist or otherwise discriminating material, unless this is necessary for the free gathering of information in the context of the performance of tasks and the user has obtained permission for this from the administrator.

3.11. The user is at any rate not allowed to send or store threatening, (sexually) intimidating, (child) pornographic or racist or otherwise discriminating email messages.

3.12. Email messages from and to the University are checked for malware (viruses and suchlike) and spam under the responsibility of the director ICTS. If necessary, contaminated messages are removed or rid of malware.

3.13 In using the University's email facility the user must use as sender an email address provided to the user by the University. The user is not allowed to make the email address available to others as send address.

3.14. The user is not allowed to read, copy, change or delete email messages intended for others, unless given explicit permission for this by the addressee, of if this takes place in the context of the directed research as referred to under clause 8.

4. Back-ups

4.1. Without a notice to the contrary from ICTS, the user may assume that the back-up procedures at the University will continue to generate reliable back-ups. Should the user use media for data storage that do not provide a standard back-up facility, he is to take care of this himself, if necessary in consultation with ICTS.

5. ICT and the use of internet by employees

5.1. The employee shall use ICT and the internet as part of the performance of his or her tasks.

5.2. The employee may make limited use of ICT and the internet for private purposes, provided this does not interfere with the employee's daily activities or the activities of other persons and these other persons do take offence at these activities.

5.3. The use of ICT and the internet by the employee for secondary duties is only allowed if and insofar as the administrator has given written permission for this.

5.4. Employees 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 employees living on the campus.

6. General supervision

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

6.2. CERT-UT may investigate traffic date in case of a security incident with the only purpose of finding and removing the cause of the incident or limiting the consequential damage of the incident. In this context CERT-UT may impose temporary restrictions upon the user in his or her access to certain ICT facilities. The user is to cooperate in this investigation by providing relevant data and complying with the instructions by CERT-UT.

6.3. Traffic data about the use of ICT and the internet are in principle kept no longer than six months. In the event of a directed investigation as referred to in clause 8, these data can be stored for a longer period, until the necessity for this no longer exists.

6.4. The ICT officer has an obligation to observe secrecy with regard to data on the use of ICT and the internet which are traceable to persons.

7. Directed investigation

7.1. In case of a suspicion of use in violation with the Code of Conduct the user in question will be called to account for his/her behaviour by the administrator as soon as possible.

7.2.1. Directed investigation into a person takes place if there are legitimate suspicions of, or if it has been established that an incorrect use as referred to in the clauses 3, 5 and 6 of this Code of Conduct has taken place. The main purposes of directed investigation are:

- establishing improper use of ITC and the internet;
- checking agreements made on the (prohibited) use;
- checking whether company secrets are sufficiently protected and are not or have not been made public;
- preventing negative publicity about the University

7.3. Directed investigation takes place after a written instruction from the Executive Board to the director ICTS and is carried out by a designated ICT officer. The instruction of the Executive Board is to state the reason for performing the investigation and why – if appropriate – the user is only informed of the investigation afterwards.

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

7.5. Only in the event of compelling reasons directed investigation into the content of email messages and stored files takes place. These reasons are stated in the written instruction 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 user in relation to whom an investigation as referred to in clause 7.3. takes place, will be informed in writing by the Executive Board as soon as possible about the reason, implementation and result of the investigation. The user is given the opportunity to provide an explanation in regard of the data found. Providing information to the user is postponed if this harms the investigation.

7.8 Items that do not belong on ICT workplaces and computer systems of the University, such as illegal software, films and music, are removed on the instruction of the administrator. The user will be informed about this in advance, unless this impedes the investigation.

8. Sanctions

8.1. If the user acts in violation of the Code of Conduct the Executive Board may impose the following sanctions:

- limited access, whether or not temporary, to certain ICT facilities;
- temporary or definitive ban to use certain ICT facilities;
- payment of costs arising from the misuse established;
- other measures (pertaining to legal status) including measures as referred to in the Disciplinary Measures Arrangement University of Twente.

9. Liability

9.1. The University retains the right to hold the user liable for damage caused by the user as a result of the use of ICT and the internet. This also includes any compensation that a third party claims from the University as a result of actions performed by the user that are in violation of this Code of Conduct.

9.2. The University excludes all and any liability for all damage arising from the use and from not being able to (fully) use the ICT facilities of the University.

10. Final provisions

10.1. Two years after the introduction of this Code of Conduct it will be evaluated.

10.2. The Wpb is fully applicable.

10.3 This Code of Conduct came about with the consent of the University Council on 11July 2011.