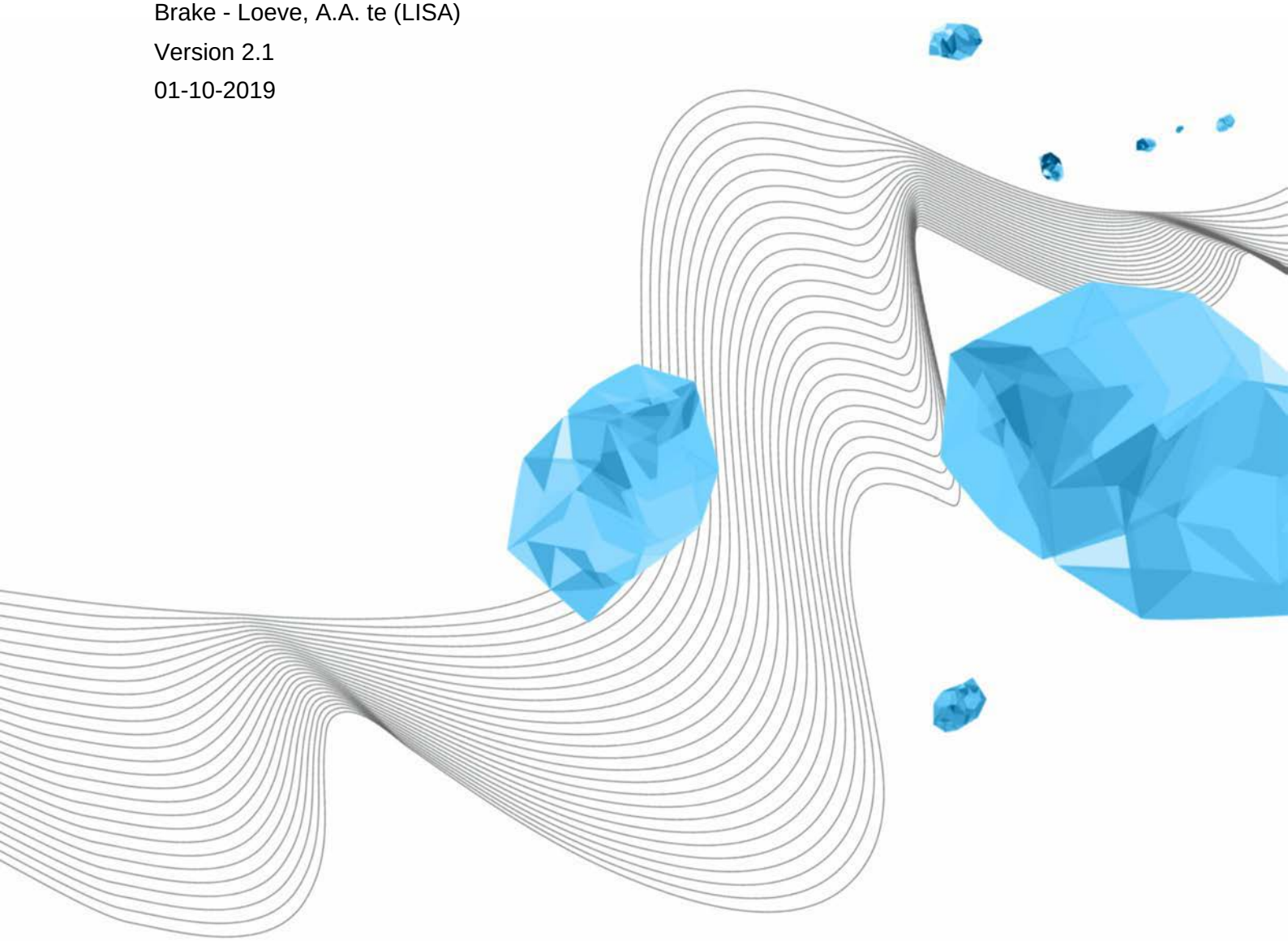
Status: Final
Date of adoption by Executive Board: 11-11-2019
Authors: Rianne te Brake/Jan Evers

# DIGITAL CODE OF CONDUCT FOR UNIVERSITY OF TWENTE STUDENTS

Brake - Loeve, A.A. te (LISA)

Version 2.1

01-10-2019



UNIVERSITY OF TWENTE.

# COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Digital code of conduct for University of Twente students

REFERNCE
UIM/181205/brk

VERSION (STATUS)
2.1

DATE
01-10-2019

AUTHOR(S)
Brake - Loeve, A.A. te (LISA)



# DOCUMENT HISTORY

| VERSION | DATE | AUTHOR(S) | COMMENTS |
|---|---|---|---|
| 1.0 | 2011 | Wim Koolhoven | Final version |
| 1.4 | 19-11-2018 | Rianne te Brake | Revised version:<br>- Structure in accordance with current SURF model<br>- Actualisation as regards privacy legislation (GDPR) and state of the art<br>- Sections deleted that have been included in independent documents |
| 1.6 | 20-12-2018 | Rianne te Brake | Comments processed, template adjusted |
| 1.7 | 15-01-2019 | Jan Evers | Comments from LISA MT processed |
| 1.8 | 06-02-2019 | Jan Evers | Comments from LISA MT and Harma Evers processed |
| 1.9 | 26-02-2019 | Jan Evers | Positive recommendation from University Operational Management Committee (UCB) (26-02-2019) |
| 2.0 | 15-04-2019 | Jan Evers | 11-03-2019 intended adoption by Executive Board (CvB)<br>10-04-2019 consultation Executive Board and University Council Finance, Staff and Operational Management committee (FPB): to UT consultative body for staff matters (OPUT) for consent and to University Council (UR) for information<br>15-04-2019 commitments from CvB to UR FPB committee processed |
| 2.1 | 01-10-2019 | Jan Evers | 24-04-2019 UR: positive recommendation with addition of 1. analysis based on UT account only, 2. data management/processing based on legislation and regulations<br>11-11-2019 adopted by CvB |

# DISTRIBUTION LIST

| VERSION | DATE | AUTHOR(S) | DISTRIBUTED TO |
|---|---|---|---|
| 1.4 | 22-11-2018 | Rianne te Brake | Jan Evers, Henk Swaters, Marc Berenschot, Peter Peters, Erna van der Zandt, Wim Olijslager (security & privacy overleg) |
| 1.6 | 20-12-2018 | Jan Evers | MT LISA |
| 1.7 | 15-01-2019 | Jan Evers | MT LISA, HR – Harma Evers |
| 1.8 | 06-02-2019 | Jan Evers | UCB |

| | | | |
|---|---|---|---|
| 1.9 | 27-02-2019 | Jan Evers | CvB |
| 2.0 | 15-04-2019 | Jan Evers | For consent to UR of 24-04-2019<br>For information to OPUT of 27-06-2019 |
| 2.1 | 01-10-2019 | Jan Evers | CvB, for adoption |

# TABLE OF CONTENTS

# 1 SOURCE REFERENCES

The Digital code of conduct for students of the University of Twente was based on the Acceptable use Policy model for students of higher education, a joint product of SURFnet and SURFibo. This publication is available under the Creative Commons Attribution 3.0 Netherlands licence[1].

# 2 INTRODUCTION

The University of Twente, hereinafter referred to as “the University”, offers its own students and visiting students the opportunity to use the internet for study purposes. In addition, an email box and possibilities for storing files and personal study data are made available to students for personal, study-related use. The use of these facilities is subject to rules. With this in mind, students can be expected to make responsible use of the internet and ICT facilities.
This code of conduct applies to all students who have been registered with the University, who pursue an education at the University or live in a student campus dwelling and who use the ICT facilities provided by the University. This scheme also applies to former students who are subject to the Arrangement ICT-Facilities for ex-UT employees and students.

# 3 USE OF FACILITIES

Computer and network facilities, such as public computers, software licences, wireless and fixed network connections, access to email and the internet, storage capacity, printers and electronic learning environment, are made available to the student for study purposes, among other things for preparing assignments, reports and theses, monitoring the study progress, consulting sources, and communicating with lecturers and fellow students. Where the University prescribes specific systems for educational purposes, the student shall only use these systems for the relevant purposes and observe strict compliance with the limitations and requirements set.

The use of own equipment and applications on the University facilities is allowed, as long as this use complies with the rules of these Regulations and the supplier’s licence conditions. Making changes to the equipment and applications made available by the University is only allowed with separate permission from the system management department. Connecting own network equipment that allows the connection to be shared with third parties on the fixed or wireless network connections is prohibited at all times, except in the students’ dwellings.

Certain facilities are only accessible using a user name and password and/or means of authentication such as an application on a smartphone. These are personal and may not be shared with others. The system management department may set further requirements for the quality of passwords and other aspects of security. In case of suspicion of abuse of a password or means of authentication, the relevant account can be rendered inaccessible with immediate effect.

[1] www.creativecommons.org/licenses/by/3.0/nl.

# 4 INTELLECTUAL PROPERTY AND CONFIDENTIAL INFORMATION

The student shall not infringe the intellectual property rights of the University and third parties and respect the licence agreements as applicable within the University.

If the student obtains access to confidential information or privacy-sensitive information including personal data within the context of his/her study or the performance of tasks for the University, the student shall treat that information as strictly confidential.
The student shall pay special attention to taking measures as specified in these regulations if the processing of confidential information outside the University is necessary for the performance of these tasks, such as via email, in non-University cloud applications, on external storage media, or own client devices (USB devices, tablets, etc.).

If the University has drawn up instructions with regard to the safeguarding of the confidentiality and the intellectual property rights, the student shall strictly follow these.

# 5 SECURITY BY THE UNIVERSITY AND BY THE STUDENT

The University is committed to the protection of information. It therefore applies a strict security policy and takes appropriate technical and organisational measures to protect the infrastructure against loss, theft, criminal activities, loss of confidentiality, violation of privacy rights, and violation of intellectual property rights. However, there is no such thing as perfect security. This is why the University expects students to adopt a proactive attitude towards the adequate protection of their own computer and other equipment (such as smartphones or tablets). The student is at all times personally responsible for the use of his/her own equipment and the data stored on this equipment. The student shall take measures in accordance with the advice and instructions provided by the cyber safety team of the University[2]. The cyber safety team does not have any formal status and powers. The team promotes cyber safety awareness. It is made up of HR, M&C and LISA staff. The team provides its advice and instructions on the basis of adopted policies.

# 6 PRIVATE USE AND NUISANCE

Limited private use of the internet and ICT facilities is allowed. Any use, either private or for study purposes, may not interfere with the good order at the University or cause nuisance to others, may not infringe any rights of the University or third-party rights, or affect the integrity and safety of the network. Furthermore, private use is only permitted if the supplier's licence conditions allow this. The University is not obliged to make backup copies of private files or private information stored on University systems or take these into account when repairing or replacing the relevant systems. The following use is regarded as prohibited, interfering and/or causing nuisance:

[2] E.g. the Cyber safety 10-phased plan.

- consulting internet services with a pornographic, racist, discriminating, insulting or offensive content in public spaces or sending messages with a similar content;
- sending messages with a (sexually) intimidating content or messages that incite or may incite to discrimination, hatred and/or violence;
- sending messages to large numbers of receivers at the same time, sending chain letters or spreading malicious software such as viruses, worms, Trojan horses, and spyware.

Students who use a University network facility in their private accommodations with private means cannot be restricted in this use, except to the extent necessary to maintain the integrity and the safety of the network or to limit the consequences of overloading. If the University takes action in order to limit the consequences of overloading, equal kinds of traffic will be dealt with equally. The other provisions of these regulations apply in full for students who use a University network facility in their accommodations.
The use of computer and network facilities for commercial activities is only allowed with written permission from the University.

# 7 MONITORING BY THE UNIVERSITY

Monitoring of the use of the facilities only takes place in the context of enforcement of the rules from this code of conduct. For the purpose of monitoring compliance with the rules, data is collected automatically (logged). Student data is only collected and analysed on the basis of a registered account of the student on the University's ICT systems. National legislation and regulations are observed for the management and processing of this data. This data is only accessible for the controller or staff members with supervisory and/or operating tasks within the framework of a targeted investigation. This data is only made available to other staff in anonymised form, unless this is impossible for the performance of management tasks.
Particularly in case of nuisance, caused by students' equipment, the network access options may be disabled. Where possible, the student is warned in advance, so he/she will have the opportunity to cease the nuisance. If, due its urgency, this is not possible before taking the measure, the measure will be communicated as soon as possible afterwards.
In case of suspicion of any violation of rules from this code of conduct, the Executive Board (CvB) may have a targeted investigation carried out (see paragraph 8). Based on a targeted investigation, a student's email may be checked without asking permission to the student in question. Not all activities that are expressly prohibited by law have been included in this code of conduct, but a check can be made for this kind of activities, for example downloading illegal material.
When performing a targeted investigation, the University fully complies with the General Data Protection Regulation and other relevant legislation and regulations. In particular, the University protects the data recorded in the course of this investigation against unauthorised access.
E-mail messages from members of the University Council, of the faculty council and members of the programme committees acting in their capacities, are not monitored insofar as they relate to their position as a member of the employee participation committee/programme committee. This does not apply for the automated monitoring of the safety of the email traffic and the network.

# 8 TARGETED INVESTIGATION

In case of grave suspicions of any violation of this code of conduct by students, the University will be entitled to carry out a targeted investigation. A targeted investigation always requires an assignment from the CvB. The University guarantees that any targeted investigation will be carried out with due care.

# 9 CONSEQUENCES OF VIOLATION

In case of actions contrary to these Regulations or the generally applicable statutory regulations, the Executive Board of the University may take measures, depending on the nature and the seriousness of the violation.
These measures include a warning, a temporary exclusion from or limitation of the facilities (for a maximum of one year), and, in extreme cases, termination of the registration as a student. With the exception of a warning, measures cannot be taken solely on the basis of an automated processing of personal data, such as an observation of an automatic filter or automated blocking. This always requires human assessment. Nor will any measures be taken without giving the student the opportunity to state his/her point of view.
In derogation from the above, the University may temporarily block the relevant facility in case of an (automated) observation of nuisance or a security risk.
This blockade will be maintained for no more than one week, or shorter if the cause has been eliminated to the satisfaction of the system management department. If after a week the system management department fails to see any improvement, it may decide on a longer blockade. In the event of repeated occurrence of the cause, measures may be taken.

# 10 FINAL CLAUSES

This code of conduct is evaluated every other year. Changes can only be implemented after the University Council has consented thereto. The Executive Board may consider feedback of students before implementing the changes.
In cases for which this code of conduct does not provide, the Executive Board will decide.
This code of conduct replaces the Code of Conduct for use of ICT and the internet by students of the University of Twente 2011.