

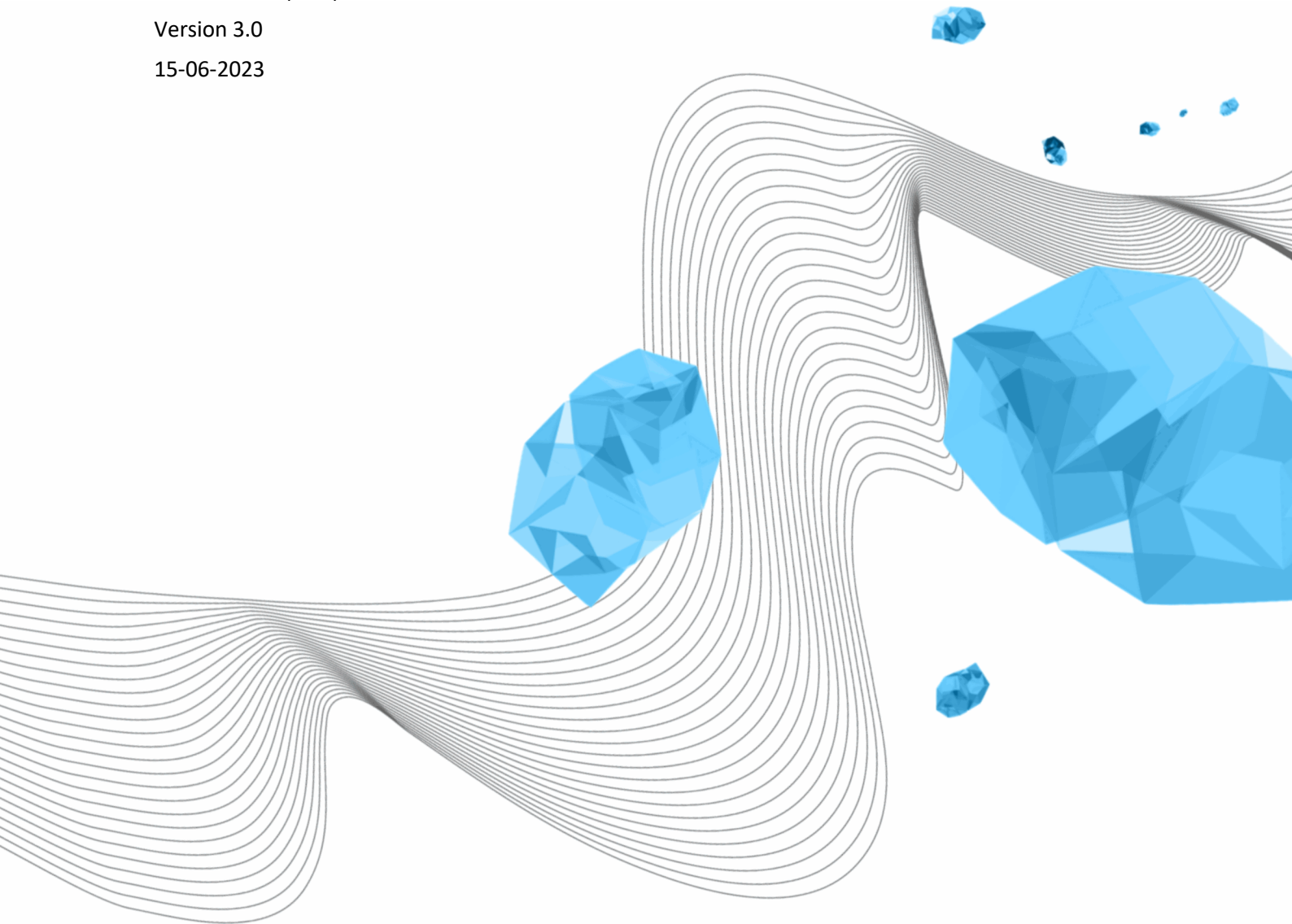
Status: Final  
Date adoption by Executive Board: 11-11-2019  
Revised: 15-06-2023  
Approved MT-LISA: 10-07-2023

# DIGITAL CODE OF CONDUCT FOR UNIVERSITY OF TWENTE STUDENTS

H.W.Swaters (LISA)

Version 3.0

15-06-2023



## COLOPHON

### ORGANISATION

Library, ICT Services & Archive

### TITLE

Digital code of conduct for University of Twente students

### ATTRIBUTE

LISA-381

### VERSION (STATUS)

3.0

### DATE

15-06-2023

### AUTHOR(S)

H.W.Swaters (LISA)

### COPYRIGHT

© University of Twente, The Netherlands.

*All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or made public, in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of the University of Twente.*

## DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	COMMENTS
3.0	04-07-2023	H.W.Swaters	Revised, no substantive changes. Author name changed. Next revision 2 <sup>th</sup> quarter 2023

## DISTRIBUTION LIST

VERSION	DATE	AUTHOR(S)	DISTRIBUTED TO
3.0	10-07-2023	H.W.Swaters	MT-LISA, for adoption

## REFERENCE

VERSION	DATE	AUTHOR(S)	TITLE
2.1	01-10-2019	Jan Evers	Digital code of conduct for University of Twente students

## TABLE OF CONTENTS

1	Citation.....	4
2	Introduction .....	4
3	Use of facilities .....	4
4	Intellectual property and confidential information .....	4
5	Security by the University and the student .....	5
6	Private use and nuisance .....	5
7	Monitoring by the University .....	6
8	Targeted research .....	6
9	Consequences of violation .....	6
10	Review of this Code of Conduct .....	7

# 1 CITATION

The Digital Code of Conduct for Students of the University of Twente is based on the Model Acceptable Use Policy for Students for Higher Education, a joint product of SURFnet and SURFibo. This publication is available under the Creative Commons Attribution 3.0 Netherlands license.<sup>1</sup>

# 2 INTRODUCTION

The University of Twente ('the University') offers its students and visiting students the opportunity to use the Internet for their studies. A mailbox and possibilities for storing files and personal study data are also made available to students for personal use for the benefit of the study. There are rules attached to the use of these facilities. Against this background, students can be expected to use the Internet and ICT responsibly.

This code of conduct applies to every student who is enrolled at the University, is studying at the University or occupies a student campus residence and who uses the ICT facilities offered by the University. In addition, this code applies to former students who fall under the Regulation on ICT facilities for former UT students.

# 3 USE OF FACILITIES

Computer and network facilities (such as public computers, (software) -licenses, wireless and fixed network connections, email and internet access, storage capacity, printers and electronic learning environment) are made available to the student for their study, including completing assignments, reports and theses, keeping track of study progress, consulting sources and communicating with teachers and fellow students. When the University prescribes specific systems for educational purposes, the student will only use these systems for the relevant purposes and strictly comply with the restrictions and requirements set therein.

The use of own equipment and applications on the University's facilities is permitted as long as such use complies with the rules of this code and the supplier's license conditions. Making changes in equipment and applications made available by the University is only permitted with separate permission from the system administrator. Connecting your own network equipment with which the connection can be shared with third parties to the fixed or wireless network connections is prohibited at all times except in students' living spaces.

Certain facilities can only be accessed using a username and password or other means of authentication, such as an application on a smartphone. These are personal and may not be shared with others. System administration may impose further requirements on password quality and other security aspects. If a suspected misuse of credentials is suspected, the relevant account can be made inaccessible immediately.

# 4 INTELLECTUAL PROPERTY AND CONFIDENTIAL INFORMATION

The student does not infringe on the intellectual property rights of the University and third parties and respects the licensing agreements as they apply within the University.

---

<sup>1</sup> [www.creativecommons.org/licenses/by/3.0/nl](http://www.creativecommons.org/licenses/by/3.0/nl).

If, in the context of their studies or the performance of tasks for the University, the student gains access to confidential or privacy-sensitive information, including personal data, the student must treat that information strictly confidentially.

The student pays particular attention to taking measures as mentioned in this code if, in the context of carrying out these tasks, the processing of confidential information outside the University is necessary, such as by email, in non-university applications, on external storage media or own client equipment (USB devices, tablets, etc.).

If the University has drawn up regulations about guaranteeing confidentiality and intellectual property rights, the student must strictly follow them.

## 5 SECURITY BY THE UNIVERSITY AND THE STUDENT

The University takes information security seriously. It, therefore, applies a strict security policy and takes adequate technical and organisational measures to secure the infrastructure against loss, theft, criminal activities, loss of confidentiality, violation of privacy rights and violation of intellectual property rights. Perfect security is impossible. That is why the University also expects students to proactively secure their own computers and other equipment (such as smartphones or tablets). The student is at all times responsible for the use of his own equipment and the data stored on this equipment. The student takes security measures following the advice and instructions of the cyber security team of the University.

## 6 PRIVATE USE AND NUISANCE

Limited private use of the ICT and Internet facilities is permitted. Use, whether personal or for study, must not be disturbing to the good order of the University and must not cause public inconvenience to others, infringe the rights of the University or third parties or affect the integrity and security of the network. In addition, private use is only permitted if the license conditions of the supplier allow this. The University is not obliged to make backup copies of stored personal files or information on the University's systems or to consider this when replacing or repairing such systems.

The following applies as prohibited, disturbing and nuisance-causing use:

- consulting internet services with pornographic, racist, discriminatory, offensive or offensive content in public areas or sending messages containing such content;
- sending messages with (sexually) harassing content or messages that (may) incite discrimination, hatred or violence;
- sending messages to large numbers of recipients at once, sending chain letters or distributing malicious software such as viruses, worms, Trojan horses and spyware.

Students who use the network facilities of the University in their private living space with private means cannot be restricted from use except to the extent necessary to preserve the integrity and security of the network or to limit the consequences of overload. If the University intervenes to limit the effects of overloading, equal types of traffic will be treated equally. The other provisions of this regulation shall apply in full to students who use a network facility of the University in their accommodation.

The use of computer and network facilities for commercial activities is only permitted if the University has given written permission.

## 7 MONITORING BY THE UNIVERSITY

Control of the use of the facilities only takes place in the context of enforcement of the rules of this code of conduct. For this control, data is collected (logged) automatically. The data of students is collected and analysed exclusively based on a registered account of the student on the ICT systems of the University. National laws and regulations are adhered to when managing and processing this data. This data is only accessible to the controller or employees with a supervisory or executive task in the context of a targeted investigation. This data will only be made available to other employees in anonymised form unless this is impossible to carry out management tasks.

In particular, in the event of a nuisance caused by student equipment, network access capabilities may be disabled. If possible, the student is warned in advance so that they have the opportunity to stop the nuisance. If, due to the urgency required, this is not possible before taking the measure, the measure shall be notified as soon as possible.

In the event of suspicions of a violation of the rules of this code of conduct, the Executive Board may order a targeted investigation (see paragraph 8). Based on a targeted investigation, a student's email may be checked without the student's permission. Not all activities prohibited by law are explicitly stated in this code of conduct. However, these activities prohibited by law can be monitored. An example of this is downloading illegal material.

When conducting a targeted investigation, the University fully complies with the General Data Protection Regulation and other relevant laws and regulations. In particular, the University protects the data recorded during control against unauthorised access.

Email messages from University Council members, faculty council members and members of the programme committees in office are not checked insofar as they relate to their position as participation committee/ programme committee members. This does not apply to automated checks on the security of email traffic and networks.

## 8 TARGETED RESEARCH

In the event of severe suspicion of violating this or other codes of conduct by a student, the UT has the right to conduct a targeted investigation. An assignment from the Executive Board is always required to carry out a targeted investigation. The UT guarantees that a targeted investigation is carried out carefully.

## 9 CONSEQUENCES OF VIOLATION

In the event of action contrary to these Regulations or the generally applicable legal rules, the College of Government of the University may take measures depending on the nature and seriousness of the violation.

This includes a warning, a temporary closure or restriction of the facilities (maximum one year) and, in extreme cases, a termination of registration as a student.

Measures (except for a warning) cannot be taken solely based on the automated processing of personal data, such as an automatic filter or blockade. This always requires human assessment. Furthermore, no action will be taken without the student being allowed to express his views.

Contrary to the previous, it is possible that the University will introduce a temporary blockade of the facility in question in the event of (automated) detection of a nuisance or a security risk.

This blockage will be maintained for a maximum of one week or less if the cause has been removed to the satisfaction of the system administrator. If the system administrator has detected no improvement after one week, they may decide on a more extended block. If the cause is repeated, measures can be taken.

## 10 REVIEW OF THIS CODE OF CONDUCT

This code of conduct is reviewed at least every two years. The following review will take place in mid-2026. There may be grounds for a mid-term review of this code of conduct. If this evaluation gives rise to it, the code of conduct will be amended sooner.

The CISO of the University of Twente is responsible for this code of conduct.

Changes will only be introduced after the University Council has agreed. The Executive Board may consider student feedback before implementing the changes.

In cases not provided for in this code of conduct, the Executive Board will decide.