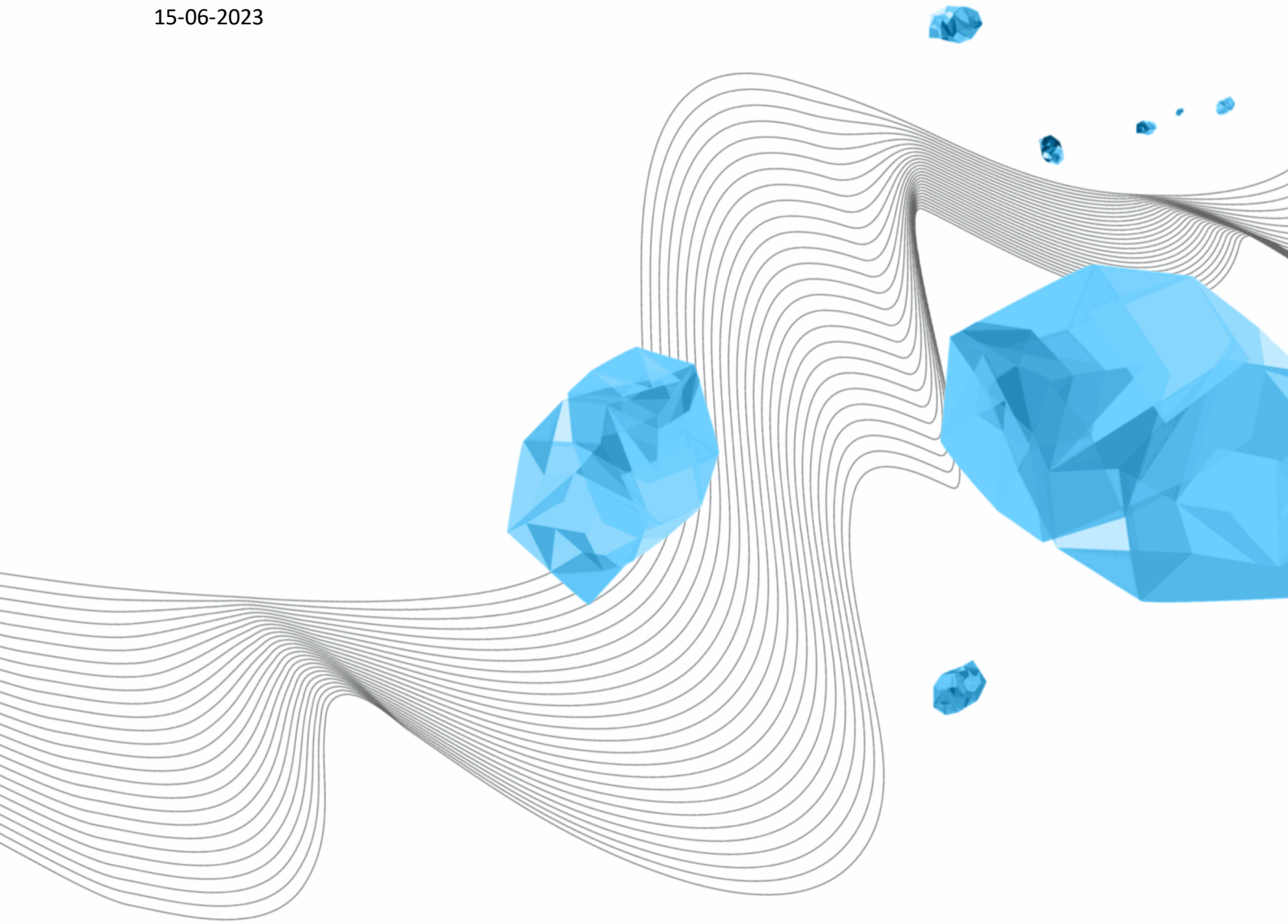
Status: Final
Date of adoption by Executive Board: 11-11-2019
Revised: 15-06-2023
Approved MT-LISA: 10-07-2023

DIGITAL CODE OF CONDUCT FOR UNIVERSITY OF TWENTE STAFF

H.W.Swaters (LISA)

Version 3.0

15-06-2023



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Digital code of conduct for University of Twente Staff

ATTRIBUTE
LISA-380

VERSION (STATUS)
3.0

DATE
15-06-2023

AUTHOR(S)
H.W.Swaters (LISA)

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	COMMENTS
2.4	15-06-2023	H.W.Swaters	Revised, no substantive changes. Author name changed. Next revision 2nd quarter 2025

DISTRIBUTION LIST

VERSION	DATE	AUTHOR(S)	DISTRIBUTED TO
2.4	10-07-2023	H.W.Swaters	MT-LISA, for adoption

REFERENCE

VERSION	DATE	AUTHOR(S)	TITLE
2.3	16-10-2019	Jan Evers	Digital code of conduct for University of Twente staff

TABLE OF CONTENTS

1 CITATION

The Digital Code of Conduct for employees of the University of Twente, from now on referred to as the University, is based on the Model Acceptable Use Policy for employees for Higher Education, a joint product of SURFnet and SURFibo. This publication is available under the Creative Commons Attribution 3.0 Netherlands license.[1]

2 BASIS FOR THE CODE OF CONDUCT

The use of the internal computer network and the public computer network (internet) and ICT facilities made available by the University is necessary for (many of) the employees of the University to be able to do their work correctly. There are risks associated with the use of these facilities. To reduce these, the University's rules of conduct bind employees. Against this background, employees are expected to use the internet and ICT facilities responsibly.

With this code of conduct, the University sets rules regarding the desired use of these assets. The aim is to balance responsible and safe ICT and internet use and the employee's privacy.

Social media such as Facebook, LinkedIn and Twitter are becoming increasingly important but can also impact the University. That is why the University also sets specific rules here.

As an employer, the University is authorised to set rules regarding work performance and good order in the workplace, as follows from the law. In addition, the "Obligations of employer and employee", as stated in the Collective Labour Agreement for Dutch Universities, are entirely in force:

- The employer is obliged to do and refrain from doing all that a good employer should do and refrain from doing in identical circumstances.
- The employee is obliged to perform their function to the best of their ability, to behave as a good employee and to act according to the instructions given by or on behalf of the employer.

Because the Code of Conduct provides for processing personal data and controlling employee behaviour or performance, the OPUT has the right to consent.

3 ARTICLES

ARTICLE 1. PRINCIPLES

1.1. Limited private use of the internet and ICT resources is permitted, provided that this does not interfere with the daily activities or the network of the University. However, the University is not obliged to make backup copies of private files or to make copies available when replacing or repairing relevant systems. Use for ancillary activities is only permitted if and insofar as the University has given written permission.

1.2. This code of conduct applies to everyone who works for the University, including temporary employees. In addition, this code of conduct applies to former employees who fall under the Regulation on ICT facilities for former UT staff. This code of conduct also applies to guests of employees who use the ICT facilities of the University.

1.3. The code of conduct does not apply to (guest) students; a different code has been drawn up. However, this code applies in full to students the University employs.

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

1.4. In the context of enforcing this code of conduct, the University strives for measures that limit access to privacy-sensitive information or personal data of individual employees as much as possible. Where possible, it will only check or filter automatically without giving itself or other persons insight into the behaviour of individual persons.
1.5. Each employee bears as much responsibility as possible for the responsible and safe use of the University's ICT and internet facilities.
1.6. The employee takes security measures following the advice and instructions of the Cybersecurity team of the University.

ARTICLE 2. CONFIDENTIAL INFORMATION

2.1 The employee must treat confidential and privacy-sensitive information, including personal data, to which he has access in the context of the work, strictly confidential and take sufficient measures to guarantee confidentiality.

ARTICLE 3. USE OF ICT FACILITIES

3.1 ICT facilities, including computer and network facilities, (software-) licenses, email and other ICT communication tools and the internet, are made available to employees for use in their function. Use is therefore linked to tasks arising from their role.
3.2 Private use and use for ancillary activities of these resources is only permitted as stipulated in Article 1.1 and only if the license conditions of the supplier allow this.
3.3 The employee must always handle login details assigned to him personally and any additional means of authentication (such as smart cards and tokens) with care. The employee may not share personal passwords and other authentication methods. In case of a suspicion of password misuse, the system administration can make the account inaccessible.
3.4 The University may prescribe systems or applications for teaching, research and other business purposes, such as an electronic learning environment, an email system, (mobile) applications (apps) or multimedia services. Employees will only use these systems for relevant purposes and strictly comply with the restrictions and requirements.
3.5 Use of the facilities (private or not) must not disturb the good order at the University. It must not cause a nuisance to others, infringe on the rights of the University or third parties or affect the integrity and security of the network.
At least forbidden for every use (private or not) of ICT facilities is:
- visiting sites or sending messages containing pornographic, racist, discriminatory, threatening, insulting or offensive content, unless this is necessary for the free collection of information in the context of the performance of their function and permission has been obtained from the administrator;
- sending messages with (sexually) harassing content;
- sending messages that (may) incite discrimination, hatred or violence;
- sending chain letters, spam or malicious software such as viruses, Trojan horses or spyware;
- the use of filesharing or streaming services in such a way that it may compromise the availability of ICT facilities.

3.6 For private email, the employee preferably uses a different email address than the one provided by the University, within the limits of article 1.1. The University will not block or monitor access to other email services.
3.7 The employee preferably provides a private email address to the University, among other things, to manage his account.
3.8 Upon termination of employment, the employee is obliged to hand in the University's equipment, including the corresponding access codes.
3.9 The connection of active network components (such as access points and routers) is not permitted without written consent from LISA.

ARTICLE 4. USE OF SOCIAL MEDIA

4.1 The University supports open dialogue, exchanging ideas, and sharing the employee's knowledge with colleagues and third parties via social media. If this concerns work-related topics, the employee must ensure that the profile and content align with how they would present themselves in text, image and sound to colleagues and students.

4.2 Administrators, managers, executives and others who promote policy or strategy or perform a representative function on behalf of the University have a special responsibility when using social media, even if the content is not directly related to their work. Based on their position, they must consider whether they can publish in a personal capacity.

4.3 This article also applies if employees participate in social media from private computers or internet connections, but only insofar as it concerns participation that may affect the work.

4.4 Upon termination of employment, the employee transfers work-related social media accounts to the University.

ARTICLE 5. MONITORING AND CONTROL

5.1 Control of the use of ICT facilities only takes place in the context of enforcement of the rules of this code of conduct.

5.2 Data is collected (logged) automatically to check compliance with the rules. The data of employees is collected and analysed exclusively based on a registered account of the employee 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.

5.3 In the event of suspicion of violating the rules of this code of conduct, the Executive Board may order an investigation (see Article 6.1). Based on a targeted investigation, an employee's email may be checked without asking the employee'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.

5.4 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 the investigation against unauthorised access.

5.5 Targeted investigations in the case of members of a participation body, OPUT members and their advisers, company doctors, HR officers and anyone entitled to invoke confidentiality under the law are always carried out by an external (forensic) investigation agency.

5.6 In the event of long-term illness, unexpected long-term absence or gross negligence of the employee, but only if this constitutes a compelling reason of business interest for access, the University is entitled to provide a replacement/manager with access to the employee's files or mailbox. This is only permitted if it can be demonstrated that obtaining permission from the employee is impossible or the business interest is so essential that consent cannot be requested after approval from the Executive Board. However, the replacement/manager may not gain access to folders marked as private, emails recognisable as private, or emails sent to or from members of a participation body, from OPUT members and their advisors, company doctors, HR officers and from anyone who is entitled to invoke confidentiality under the law – if those emails related to their role mentioned here. Before the replacement or manager receives access, the University engages a member of CERT-UT, a confidential advisor or an HR advisor to check the relevant information of the employee to recognise and shield private information. In the case of emails sent to or from members of a participation body, from OPUT members and their advisers, company doctors, HR officers and from anyone who is entitled to invoke confidentiality under the law, these emails will be examined and protected by an external forensic investigation agency if those emails related to their role mentioned here. The forensic investigation agency also does the shielding of private information.

ARTICLE 6. TARGETED RESEARCH

6.1 In the event of severe suspicions of a violation of this, or other code of conduct by an employee, the University has the right to conduct a targeted investigation. A targeted investigation means examining existing, already available information to determine whether and to what extent there has been a violation of the code of conduct. An assignment from the Executive Board is always required to carry out a targeted investigation. The University guarantees that a targeted investigation is carried out carefully.

ARTICLE 7. CONSEQUENCES OF VIOLATION

7.1 In the event of a breach of this code of conduct, the Executive Board may, depending on the nature and seriousness of the infringement (proportionality), impose one or more of the following sanctions:
   a. temporary or permanent restriction on access to certain ICT facilities;
   b. temporary or permanent ban on the use of certain ICT facilities;
   c. payment of costs resulting from the abuse detected;
   d. warning or reprimand or dismissal.

7.2 Sanctions (except for a warning) cannot be taken solely based on the automated processing of personal data, such as an automatic filter or blockade.

7.3 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 nuisance or a security risk.

7.4 Sanctions are never taken without a hearing. A written report is made of this and provided to the employee.

4 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-2025. 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 OPUT has agreed. In cases not provided for in this code of conduct, the Executive Board will decide.