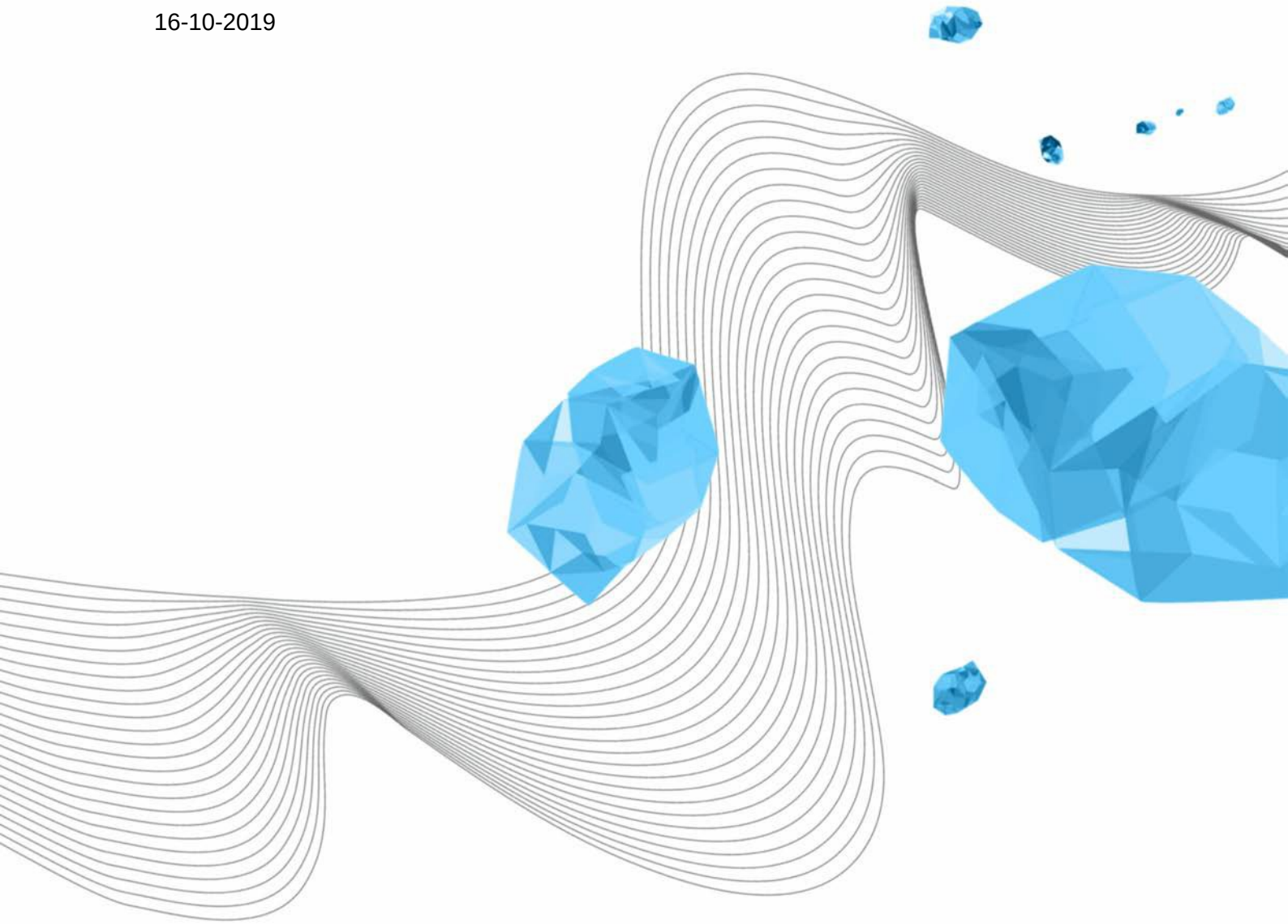
Status: Final
Date of adoption by Executive Board: 11-11-2019
Authors: Rianne te Brake/Jan Evers

DIGITAL CODE OF CONDUCT FOR UNIVERSITY OF TWENTE STAFF

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

Version 2.3

16-10-2019



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Digital code of conduct for University of Twente staff

REFERENCE
UIM/181204/brk

VERSION (STATUS)
2.3

DATE
16-10-2019

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

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	COMMENTS
1.0	2009	Wim Koolhoven	Final version
1.1	15-06-2018	Rianne te Brake	Revised version: - Structure in accordance with current SURF model - Actualisation with regard to privacy legislation (GDPR) and state of the art - Sections deleted that have been included in independent documents
1.6	04-12-2018	Rianne te Brake	Templates adjusted, comments processed
1.8	15-01-2019	Jan Evers	Comments from LISA MT processed
1.9	06-02-2019	Jan Evers	Comments from LISA MT and Harma Evers processed (inter alia WNRA check)
2.0	26-02-2019	Jan Evers	Positive recommendation from University Operational Management Committee (UCB) (26-02-2019)
2.1	15-04-2019	Jan Evers	11-03-2019 intended adoption by Executive Board (CvB) 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 15-04-2019 commitments from CvB to UR FPB committee processed 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
2.2	28-08-2019	Jan Evers	Changes following questions asked by OPUT
2.3	16-10-2019	Jan Evers	Targeted investigation and access to email of UR members, OPUT members, etc. external. (5.5 and 5.6) – following OPUT meeting 16-10-2019 written consent from OPUT (letter with ref. 2019/10/001) 11-11-2019 adopted by CvB

DISTRIBUTION LIST

VERSION	DATE	AUTHOR(S)	DISTRIBUTED TO
1.1	15-06-2018	Rianne te Brake	Jan Evers, Henk Swaters, Peter Peters, Marc Berenschot, Erna van der Zandt, Wim Olijslager (security & privacy consultation)
1.6	06-12-2018	Rianne te Brake	Jan Evers, Henk Swaters, Peter Peters, Marc Berenschot, Erna van der Zandt, Wim Olijslager
1.8	15-01-2019	Jan Evers	MT LISA, HR – Harma Evers
1.9	06-02-2019	Jan Evers	UCB
2.0	27-02-2019	Jan Evers	CvB
2.1	15-04-2019	Jan Evers	For consent to OPUT of 27-06-2019 For information to UR of 24-04-2019
2.2	28-08-2019	Jan Evers	For consent to OPUT of 19-09-2019
2.3	16-10-2019	Jan Evers	For consent to OPUT for written handling by CvB, for adoption

TABLE OF CONTENTS

1 SOURCE REFERENCES

The Digital code of conduct for staff members of the University of Twente, hereinafter referred to as the University, 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 BASIS FOR THE CODE OF CONDUCT

The use of the internal computer network and the public computer network (the internet) and ICT facilities that are made available by the University is necessary for many staff members of the University for the proper performance of their jobs. As the use of these facilities entails risks, staff members are obliged to abide by the code of conduct of the University. With this in mind, staff can be expected to make responsible use of the internet and ICT facilities.

With this code of conduct, the University sets rules regarding the desired use of these business assets. The aim is to achieve a proper balance between responsible and safe use of ICT and internet and the privacy of the staff member.
The use of social media like Facebook, LinkedIn and Twitter is becoming ever more important, but may also have a negative impact on the University. It is for this reason that the University sets certain rules for their use.
It follows from the law that, as an employer, the University is authorised to set certain rules with regard to the performance of the work and the good order in the workplace. In addition, the “Obligations of the employer and employee”, as stated in the Collective Labour Agreement of Dutch Universities, apply in full:

- The employer is obliged to do and omit everything which a good employer should do and omit in similar circumstances.
- The employee is obliged to perform his/her position to the best of his/her abilities and to act in accordance with the instructions provided by or on behalf of the employer.

As the Code of Conduct also concerns the processing of personal data and/or monitoring of behaviour and/or performance of staff members, the UT consultative body for staff matters (OPUT) has the right of consent.

3 ARTICLES

ARTICLE 1. STARTING POINTS

1.1. Limited private use of the internet and ICT facilities is allowed, provided that this does not interfere with the daily work or the network of the University. However, the University is not obliged to make backup copies or make copies available in case of repair or replacement of the relevant systems. Use for ancillary activities is only allowed if and insofar as the University has given permission in writing for this.
1.2. This code of conduct applies for everyone who is working for the University, which also includes agency workers and temporary workers. This code of

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

conduct also applies to former staff members who are subject to the Arrangement ICT-Facilities for ex-UT employees and students. Furthermore, this code of conduct also applies to guests of staff members who use the ICT facilities of the University.

1.3. The code of conduct does not apply for guest students or regular students: a separate code of conduct has been drawn up for them. This code of conduct does apply in full, however, for students who are also employed with the University.

1.4. Within the framework of the enforcement of this code of conduct, the University aims for measures that limit as much as possible access to privacy-sensitive information or personal data of individual staff members. Where possible, it will only apply automated monitoring or filtering without providing itself or other persons with insight into behaviour of individual persons in the process.

1.5. Each staff member is – as far as possible – personally responsible for the responsible and safe use of the ICT and internet facilities of the University.

ARTICLE 2. CONFIDENTIAL INFORMATION

2.1 The staff member shall maintain the strict confidentiality of confidential and privacy-sensitive information including personal data, to which he/she has access in the performance of his/her duties, and take sufficient measures to safeguard the confidentiality.

2.2 The staff member shall take security 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.

ARTICLE 3. USE OF ICT FACILITIES

3.1 ICT facilities, including computer and network facilities, (software) licences, email and other ICT means of communication and the internet, are made available to the staff member for use in the context of his/her job. This use is therefore related to tasks arising from this job.

3.2 Private use and use for ancillary activities of these facilities is only permitted as specified in article 1.1, and only if the supplier's licence conditions allow this.

3.3 At all times, the staff member shall handle the login details and any additional means of authentication (such as smart cards and tokens) that he/she has personally been provided with, with due care. Personal passwords and means of authentication may not be shared. In case of suspicion of abuse of a password, the system management department may render the account concerned inaccessible with immediate effect.

3.4 The University may prescribe systems or applications, such as an electronic learning environment, an email system, mobile applications (apps) or multimedia services, for purposes of education or research or other business purposes. The staff member shall use only these systems for the relevant purposes and strictly comply with the limitations and requirements set for use.

3.5 Use of the facilities, whether or not private, may not interfere with the good order at the University and may not cause nuisance to others, infringe any rights of the University or third parties, or affect the security of the network. In any case, for any use – whether or not private – of ICT facilities, the following is forbidden:

- visiting sites or sending messages with pornographic, racist, discriminating, threatening, insulting or offensive content, unless this is necessary for the free information gathering in the context of the performance of the job and permission for this has been obtained from the manager;

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

- sending messages with a (sexually) intimidating content;
- sending messages that incite or may incite to discrimination, hatred and/or violence;
- sending chain letters, spam or malicious software such as viruses, Trojan horses or spyware;
- the use of file sharing and/or streaming services to such an extent that this may endanger the availability of the facilities.

3.6 The staff member preferably uses an email address other than the email address provided by the University for his/her private email, within the limits set in article 1.1. The University will not block or specifically monitor access to other email services.

3.7 The staff member preferably provides the University with a private email address, among other things for the management of his/her account. For example, in case of a forgotten password, the resetted password will be sent to the private email address. If this is not available, the staff member will have to go to the service desk with proof of ID. The private email address is also used by HR in the course of the appointment procedure.

3.8 On termination of the employment, the staff member is obliged to hand in the University's equipment, including the associated access codes.

3.9 Connecting active network components (such as access points and routers) is not allowed without the written permission from LISA network management.

ARTICLE 4. USE OF SOCIAL MEDIA

4.1 The University endorses the open dialogue and the exchange of ideas and the sharing of the ideas of staff members with colleagues and third parties through social media. If this concerns work-related topics, the staff member shall ensure that the profile and content are in line with the manner in which he/she would present himself/herself to colleagues and students in text, images and sound.

4.2 Board members, managers, superiors and others who propagate policies or strategies on behalf of the University or who have a representative position, have a special responsibility when using social media, even if the content is not directly related to their work. In view of their position, they should consider publishing in a personal capacity.

4.3 This article also applies if staff members participate in social media from their private computers or internet connections, but only insofar as this participation may affect the work.

4.4 On termination of the employment, the staff member hands over work-related social media accounts to the University.

ARTICLE 5. MONITORING AND SUPERVISION

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

5.2 For the purpose of monitoring compliance with the rules, data is collected automatically (logged). Staff data is only collected and analysed on the basis of a registered account of the staff member 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.

5.3 In case of suspicion that rules from this code of conduct are violated, the Executive Board (CvB) may have a targeted investigation carried out (see article 6.1). Based on a targeted investigation, a staff member's email may be checked without asking permission to the staff member 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.

5.4 When performing a targeted investigation, the University shall fully comply 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.

5.5 In case of members of an employee participation body, OPUT members and their advisers, of occupational physicians, of HR officials and of anyone who may invoke confidentiality under the law, a targeted investigation will always be carried out by an external (forensic) research agency.

5.6 In the event of long-term illness, unexpected long-term absence or gross negligence of the staff member, but only if this results in a compelling reason for access in the interest of the business, the University is entitled to give a substitute/manager access to the staff member's files or email box. This is only permitted if it can be demonstrated that obtaining permission from the staff member is impossible or the business interest is of such a compelling nature that permission cannot be asked, and after permission from the Executive Board. However, the substitute / manager may not access files that have been marked as private, emails that are recognisable as private, or emails sent to or received from members of an employee participation body, OPUT members and their advisers, occupational physicians, HR officials and anyone who may invoke confidentiality under the law – if these emails relate to their aforementioned capacities. Before granting access to the substitute or manager, the University will engage a CERT-UT staff member, a confidential adviser and/or an HR adviser to check the staff member's relevant information in order to recognise and block private information. In case of emails sent to or received from an employee participation body, OPUT members and their advisers, occupational physicians, HR officials and anyone who may invoke confidentiality under the law, these emails are investigated and blocked by an external forensic research agency if they relate to their aforementioned capacities. The forensic research agency will also block private information in that case.

ARTICLE 6. TARGETED INVESTIGATION

6.1 In case of grave suspicions of any violation of this or any other code of conduct, the University will be entitled to have a targeted investigation carried out. A targeted investigation is taken to mean investigating the existing information that is already available in order to establish whether there has been a violation of the code of conduct and if so, to what extent. A targeted investigation always requires an assignment from the CvB. The University guarantees that any targeted investigation will be carried out with due care.

ARTICLE 7. CONSEQUENCES OF VIOLATION

7.1 In case of actions contrary to this code of conduct, the Executive Board may, depending on the nature and the seriousness of the violation (proportionality), impose one or more of the following sanctions:
   a. temporary or definitive limitation of the access to certain ICT facilities;
   b. temporary or definitive prohibition on the use of certain ICT facilities;
   c. payment of the costs ensuing from the observed abuse;
   d. warning or reprimand or dismissal.

7.2 With the exception of a warning, sanctions cannot be imposed solely on the basis of an automated processing of personal data, such as an automatic filter or automated blocking.

7.3 In derogation from the above, the University may block the relevant facility, temporarily or otherwise, in case of (automated) observation of nuisance or a security risk.

7.4 Sanctions will never be imposed without hearing both sides of the argument. A written report of this will be drawn up, and this report will be provided to the staff

member.

ARTICLE 8. FINAL CLAUSE

8.1 This code of conduct is evaluated every other year.
8.2 In cases for which this code of conduct does not provide, the Executive Board will decide.
8.3 This code of conduct replaces the University of Twente Code of Conduct for use of ICT and the Internet 2009.