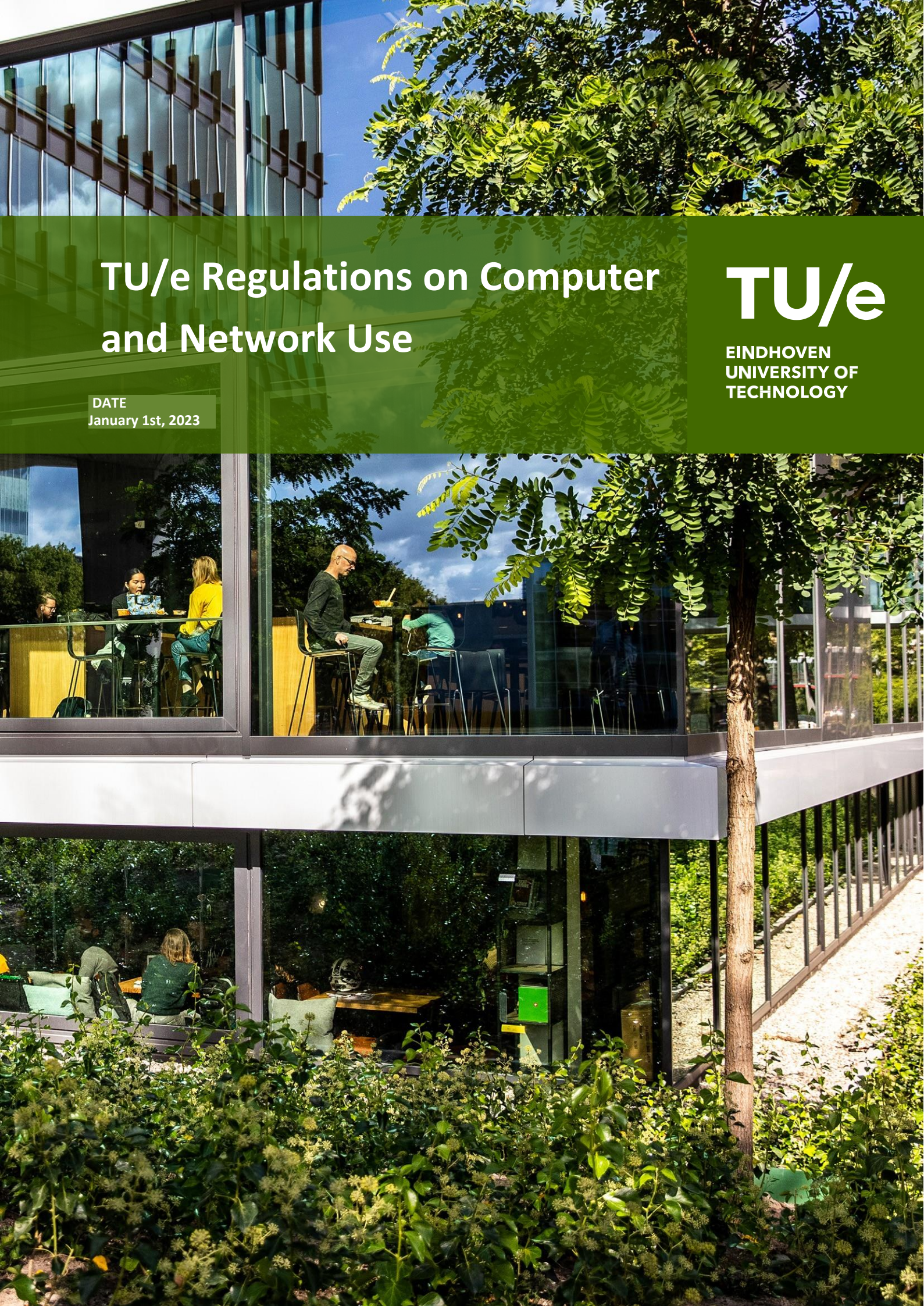

TU/e Regulations on Computer and Network Use

DATE
January 1st, 2023

TU/e
EINDHOVEN UNIVERSITY OF TECHNOLOGY

TU/e Regulations for Computer and Network Use

Summary

Students and employees use computers and the internet almost daily for their studies and work. TU/e is committed to facilitating this by providing good ICT equipment and facilities for use by students and staff. There is always a risk, however, that improper use will be made of these equipment and facilities. For that reason, it is important to have rules of conduct in place for the use of TU/e ICT equipment and facilities.

TU/e has laid down these rules of conduct in its 'Regulations for Computer and Network Use'. These Regulations set out how you as a user (student or employee of TU/e or a third party) may use the available ICT equipment and facilities, how liability is regulated and what measures TU/e will take in case of misuse of the ICT equipment and facilities.

Ground rules

The conditions and procedures relating to the use of the ICT equipment and facilities are laid out in detail in the Regulations referred to above. With a healthy dose of common sense and observance of certain 'ground rules', you will find that most aspects are easily covered, however. We have listed the main rules below:

1. You may, to a limited extent, use the ICT equipment and facilities that are provided by TU/e for private purposes. It goes without saying that you should ensure this does not obstruct or interfere with your normal work (and that of others), and that you also observe the usual standards of decency as well as all applicable legal standards when using TU/e ICT equipment and facilities.
2. Make sure your activities do not overload the ICT equipment and facilities. Don't send large numbers of messages or messages that are so large they might slow down the system, for example.
3. Keep your user name, password and email address for personal use only, and don't give these details to anyone else. Also, be careful not to leave a computer you are logged into unattended. You will be held personally liable in the event your account is misused.
4. Make sure that messages you send are not offensive, insulting, discriminatory, or otherwise inappropriate, unauthorized or unlawful.
5. It goes without saying that you should not use ICT equipment and facilities for any illegal activities, such as hacking, breaking or cracking security codes, committing fraud, and illegally downloading or copying files.
6. You should, of course, never send any chain letters, advertising messages or any other type of "spam" message.
7. Don't reset any system setting of the TU/e equipment and facilities, and handle them with due care.
8. You may not use the hardware and software provided to you by TU/e for advertising or commercial purposes, and you may not make them available to any third party. Should you do so in spite of this prohibition, and TU/e is fined as a result, then the fine will be passed on to you.
9. If you use any private device for work or study-related activities, then you are bound by the TU/e Mobile Device and Teleworking Policy. The text of this Policy can be found on the intranet.

Procedures and measures

TU/e may take action against any suspected improper use of the TU/e computer and network facilities. TU/e is required, for example, under certain circumstances to make data and/or files from a computer available to the authorities if requested to do so under any legal basis. TU/e may also launch an investigation if it suspects unauthorized use of the user name, password or data. As a student or employee of TU/e, you are required to cooperate in any such investigation. TU/e will naturally comply with the provisions of the General Data

Protection Regulation when conducting any investigation.

TU/e shall be compelled to take action in response to any confirmed instance of unauthorized use of the TU/e ICT equipment and facilities. Reports of misuse are made and handled in the manner described in these Regulations. Sanctions vary, depending on the seriousness of the violation.

Additional information

The full text of the Regulations on Computer and Network Use are set out below.

TU/e Regulations on Computer and Network Use

The Executive Board of Eindhoven University of Technology (TU/e), having regard to Section 7.57h of the Higher Education and Research Act (Wet op het hoger onderwijs en wetenschappelijk onderzoek, 'WHW') and the Regulations for University Buildings, Sites and Other Facilities,

RESOLVES to withdraw:

- The TU/e Regulations for Computer and Network Use 2012;

and **TO ADOPT**:

- The TU/e Regulations for Computer and Network Use 2022, which read as follows:

Article 1 Glossary of Terms

The terms used in these Regulations have the following meanings:

Managing Director:	The director of operations or the head of the management unit who is mandated by the Executive Board for the management of the unit concerned.
Responsible Authority:	The Executive Board of TU/e is the Responsible Authority. The Executive Board may assign the role and tasks of the Responsible Authority to the Faculty Board, the Managing Director or any other person or body by the granting of a mandate.
CERT	Computer Emergency Response Team
CGC:	the 'Commissie Gedragscode Computergebruik' (Committee on Code of Conduct for Computer Use)
Third Party:	a User who is hosted by TU/e, or a temporary employee, such as an agency worker, intern or externally contracted staff.
ESA:	Education and Student Affairs of the TU/e.
User:	a natural person who uses the ICT equipment and facilities with the consent of the Responsible Authority, as shown by the issuing by the Responsible Authority of a user name, email address and/or other access code or by acceptance of the conditions of use in the case of the guest (WiFi) network.
ICT equipment:	the computer and network facilities provided by or on behalf of TU/e, including electronic equipment, such as computers and desktop computers, laptops, notebooks, tablets, cell phones and printers, and software, licenses such as software, computer operating systems and other computer and/or network facilities, such as the physical and WiFi network (the secure network and guest network).
ICT facilities:	the means provided by or on behalf of TU/e for electronic data exchange, including, but not confined to, (access to) the internet, intranet, email, library information systems, social media accounts and/or chat groups and all other electronic facilities whether or not accessible through the use an access code or a link, as well as connection facilities for electronic devices.

LIS:	Library and Information Services of TU/e.
Report:	a notification submitted in writing (including by electronic means) concerning incorrect or unauthorized use of the ICT equipment and facilities by a User.
Misuse:	use of the ICT equipment and facilities in breach of these Regulations and/or a relevant legal rule, unwritten or otherwise, irrespective of whether such misuse is of a serious or less serious nature, as referred to in Annex 1 to these Regulations.
Program Director:	The officer designated by the Executive Board as being tasked with implementation of these Regulations for the students of the program concerned.
OST	Operational Security Team
Secretary of the CGC:	the LIS Director or a mandatary appointed by him/her, and also in that capacity Secretary of the CGC.
Social media	for example, but not confined to, Facebook, YouTube, Instagram, Skype, WhatsApp, Twitter or LinkedIn.
Student:	a user who is enrolled as a student, whether full-time or part-time, at TU/e.
Regulations:	these TU/e Regulations for Computer and Network Use.
Chairperson of the CGC:	The ESA Director or a mandatary appointed by him/her, and also in that capacity Chairperson of the CGC.
Employee:	a user with a permanent or temporary employment contract with TU/e in accordance with the Collective Labor Agreement for Dutch Universities (CAO Nederlandse Universiteiten).

Article 2 Applicability of these Regulations and Authorization of Use

2.1 These Regulations apply to all use of ICT equipment and facilities provided by TU/e, irrespective of where and how they are used or the location or manner in which users log in.

2.2 These Regulations apply to all users who work, study, and/or use the ICT equipment and facilities at TU/e, irrespective of whether or not they are physically present at TU/e at the time of such use.

2.3 Only Users are authorized to use the ICT equipment and facilities.

2.4 Users are required, if necessary, to identify themselves when using the ICT equipment and facilities by means of the user name and/or email address issued to them by the Responsible Authority, where applicable together with the password. Users shall keep their user name and password strictly confidential and not disclose the user name or the password to any other party.

2.5 If requested to do so by the Responsible Authority, a User shall immediately show his/her TU/e identification by presenting his/her campus card.

2.6 A User shall not misuse the ICT equipment and facilities provided by the Responsible Authority, as well as the user name, password and email address issued to him/her.

2.7 User names, passwords and/or email addresses are strictly personal. Users who have legitimately received a user name, password and/or email address from the Responsible Authority, or who are using them, are responsible for any and all use made of their user name, password and/or email

address, including by any other party.

Article 3 Liability

3.1 TU/e accepts no liability whatsoever for any loss or damage resulting from the use of the ICT equipment and facilities, including any and all liability in respect of the quality and/or availability of the ICT equipment and facilities and/or any information disseminated and/or obtained using the ICT equipment and facilities, unless in the event of willful misconduct or gross negligence attributable to TU/e.

3.2 The User shall be liable for any loss or damage resulting from any incorrect use, or failure to take due care when using or unauthorized use of his/her user name, password and/or email address or any other access data provided by the Responsible Authority, including such use by any other party.

3.3 The User shall be liable for any damage he/she causes to or in the ICT equipment and facilities, including damage resulting from use contrary to Article 2 and/or Article 4, unless the damage is not attributable to the User. The User shall compensate TU/e for any such damage.

3.4 In addition to the loss or damage referred to in Article 3.2 and Article 3.3, the User shall also be liable for any loss or damage sustained by TU/e and/or others resulting from the use of the ICT equipment and facilities by the User in contravention of Article 2 and/or Article 4, or otherwise resulting from failure to exercise the due care that may be expected of the User.

3.5 The User shall indemnify TU/e against any and all claims and/or demands made against TU/e by any other party in connection with any infringement of the rights of such other parties, where such infringement may be attributable to the User, also including infringement of intellectual property rights and/or wrongful acts committed toward the other parties. Claims and/or demands brought against TU/e by other parties shall be passed on to the User.

Article 4 Manner of use

4.1 The ICT equipment and facilities used by the User are intended primarily and mainly for the purposes of education and research in connection with the programs or courses for which the User is enrolled, or for the performance of the User's duties, or for the purpose for which the User is present at TU/e. The User may additionally make limited personal use of the ICT equipment and facilities, provided that such use does not obstruct or interfere with their own normal work or that of others, and that others cannot take offense at such use. Such personal use may furthermore not place a disproportionate burden on the ICT equipment and facilities of TU/e and may not infringe any licenses held by TU/e or any intellectual property rights and other rights vested in TU/e and/or other parties.

4.2 When using the ICT equipment and facilities, Users may not:

a. Perform any actions that may cause material or immaterial damage to TU/e or others;
b. Infringe any rights vested in TU/e or others;
c. Cause any nuisance or inconvenience, or disturbance of public order;
d. Perform any action that contravenes any applicable law, including those arising from laws relating to intellectual property rights, including the Copyright Act (Auteurswet), the Benelux Trademark Act (Benelux Merkenwet), the Neighboring Rights Act (Wet op de Naburige rechten), the Databases Act (Datenbankenwet) as well as rights arising from the Penal Code (Wetboek van Strafrecht), the General Data Protection Regulation or with rights arising from the Dutch Civil Code (Burgerlijk Wetboek), more specifically Article 6:162 et seq;
e. Act in any way contrary to the unwritten rules of social convention;
f. Use another person's user name, password and/or email address or other personal access data of others. Where this does happen, such use by the other person will be attributed to the rightful holder of the user name, password and/or email address or other access data;

g. Use a different or fake user name, password and/or email address, or otherwise attempt to conceal his/her identity;
h. Gain unauthorized access to another person's data, files and/or computer systems, whether or not by means of hacking, or breaking or cracking a security code (also including wardriving, sending cookies, etc.);
i. Break or crack a security measure or security code;
j. Send or post messages, notices or communications whose contents may be deemed offensive, lewd, discriminatory, inflammatory, defamatory, insulting, offensive, hurtful, improper or otherwise contrary to public order or decency or may otherwise be considered unlawful, or make such messages, notices or communications accessible by means of hyperlinks or publish such messages in any other way;
k. Send or post large numbers of messages or large messages which the User knows or could or ought to have known may cause disturbances, nuisance and/or delays within the system, or for the recipient/recipients, or make such messages accessible by means of hyperlinks or otherwise publish them;
l. Send or post unsolicited messages which the User knows or could or ought to have known are not intended for the benefit of the recipient/recipients and are not related to the study program or the function of the persons concerned, or make such messages accessible by means of hyperlinks or otherwise publish them;
m. Intentionally send or post messages, notices or communications whose contents the User knows or could or ought to have known are inaccurate or incorrect, or make such messages, notices or communications accessible by means of hyperlinks or otherwise publish them.
n. Send or post chain letters, advertising messages and similar messages, or make such messages or letters accessible by means of hyperlinks or otherwise publish them.
o. Make the ICT equipment and facilities available to other parties.
p. Run or use ICT equipment and facilities unnecessarily, preventing their use by other authorized Users. This includes not only keeping an item or items of equipment or a facility in use without the User being physically present, but also using the ICT equipment and facilities for another purpose than that described in Article 4.1.
q. Leave the ICT equipment and facilities, or leave them in an operating or open condition such that others are able to use or Misuse the Equipment or Facility.
r. Use the ICT equipment and facilities for illegal or unauthorized purposes.
s. Make changes to system and other settings of TU/e ICT equipment and facilities.
t. Infect the ICT equipment and facilities with a virus.
u. Use the ICT equipment and facilities for advertising messages and for commercial purposes. In case of infringement of this provision resulting in a penalty or fine being imposed on TU/e, the penalty or fine will be recovered from the person responsible for non-compliance with this provision.

4.3 Any use of the ICT equipment and facilities in breach of Article 4.1 and/or use as covered by Article 4.2 shall constitute Misuse.

Article 5 Management measures

5.1 LIS may, in the interest of the ICT equipment and facilities or parts thereof, or in the interest of the traffic flows across the ICT equipment and facilities, implement practical measures that may be detrimental to the User and/or the use of the ICT equipment and facilities without this giving rise to any liability on the part of TU/e.

5.2 The LIS Director is authorized at his/her discretion to make announcements regarding the provisions in Article 5.1 and/or provide explanations in relation to the measures that are implemented.

Article 6 Provision of information on the basis of Legislation and Regulations

6.1 The Responsible Authority is authorized if and when required to do so as a result of statutory regulations (including general administrative orders or bylaws, including those issued by local

authorities or bodies or organizations governed by public law) and/or judgments of a judicial authority, including those provisionally enforceable notwithstanding appeal, to make information and/or data files of a User which are stored in or are accessible by means of the ICT equipment and facilities available for inspection by, or to reproduce, download or copy (or cause to be reproduced, downloaded or copied) such information and/or files for use by a duly authorized officer; the User shall immediately comply with any such request and shall pass the copied information and/or files to the duly authorized officer.

6.2 In the event that one or more persons, relying on legislation or regulations as referred to in Article 6.1, request the Responsible Authority to allow inspection of and/or access to, etcetera the data of a User stored in the ICT equipment and facilities as provided in Article 6.1, the Responsible Authority will not comply with any such request unless and until the officer and/or officers have formally identified themselves and provided that the relevant formalities required by law or regulations have been observed.

6.3 The Responsible Authority shall comply with the provisions of the General Data Protection Regulation.

6.4 The actions undertaken by TU/e pursuant to this Article shall under no circumstances give rise to liability on the part of TU/e toward the User.

Article 7 Monitoring and Investigation in response to suspicious indications

7.1 TU/e will, in connection with enforcement of the rules laid down in these Regulations and solely for the purposes referred to in the Ground Rules (which are listed on page 2), exercise monitoring and control of the ICT equipment and facilities. Access to privacy-sensitive information or personal data of individuals will be kept to a minimum. Where possible, checks and filtering will be carried out by automated means only, without this providing any insight into individuals' behavior. A weighing of interests will always be undertaken in respect of the need to safeguard the security and integrity of the ICT equipment and facilities and the importance of protecting the User's privacy.

7.2 In the interest of safeguarding the security and integrity of the ICT equipment and facilities, the activities and data of Users of the ICT equipment and facilities will be continuously processed by automated means, on the basis of monitoring and logging. These automated procedures may, in accordance with predetermined rules, result in a system alert. This alert may indicate a need for further investigation.

7.3 Where there are reasonable grounds for suspecting a breach of the rules referred to in these Regulations or any infringement of other laws and regulations, or where a system message indicates a need for further investigation, the Responsible Authority may order that a specific investigation be carried out. 'Specific investigation' hence refers to the carrying out of an investigation into a suspected breach of these Regulations, a suspected infringement of laws and regulations, or an automated system message, involving targeted actions aimed at identifying whether a breach or infringement has actually occurred, and to what extent and with what measures the risks, if any, may potentially be mitigated.

7.4 A specific investigation may be carried out at the level of individual traffic data related to email and internet use. A specific investigation into content shall only be carried out where there are compelling reasons for doing so. The data obtained during a specific investigation shall only be accessible to system administrators of the service department concerned, or external or other analysts who are engaged to further analyze the alert. Such data shall only be made available to other administrators or staff involved in carrying out the investigation in fully anonymized form.

7.5 In urgent cases, or where necessary to avoid a risk, or the continued risk, of loss and/or damage,

the CERT may decide to implement technical measures, whether or not with the assistance of system administrators, which may include blocking access to a particular service or restricting the ability of the affected equipment to use the network, for example. Such measures will always be temporary measures, and will not remain in place for longer than is necessary. Where circumstances allow, the OST will assess in advance whether a measure is appropriate; as part of this assessment a weighing of interests will also be undertaken in respect of the need to safeguard the security and integrity of the ICT equipment and facilities and the importance of protecting the User's privacy. In urgent cases, the OST and CERT will be notified at the earliest opportunity after a measure has been implemented.

7.6 Where there are reasonable grounds for suspecting that a User is committing or has committed a breach or infringement, specific monitoring measures may be implemented for a certain period of short duration. Such monitoring will only address content where there are justified and compelling reasons for doing so.

7.7 TU/e may implement various specific measures for the purpose of ensuring compliance with these Regulations, including:

a) Monitoring aimed at avoiding negative publicity and control for system and network security purposes, to be carried out based on automated scans of content, including email filtering and virus scanners.

b) Monitoring with a view to cost and capacity management. Where such sources result in significant expenditure or inconvenience, they will be blocked or restricted without any resulting breach of confidentiality with regard to the communication in question.

c) Monitoring aimed at enhancing the security of the ICT equipment and facilities as well as avoiding cyber security incidents. This monitoring can be carried out through various means, including simulated attacks, such as security penetration testing, and social engineering, such as phishing campaigns.

7.8 The User shall cooperate fully in any investigation carried out by the Responsible Authority or on behalf of the Responsible Authority and, if necessary, shall make the ICT equipment and facilities as well as the data available, and shall additionally provide unrestricted access to the data that are accessible using the ICT equipment and facilities. The User shall, in that case, also provide access to any data which the User does not keep on the hard disk of the electronic equipment, but which can be accessed using the ICT equipment and facilities, and shall allow copies to be made of such data.

7.9 After the investigation is completed, the Responsible Authority will notify the User in writing of any irregularities it has found, together with a brief description of the reasons for the investigation. If no irregularities are found, the Responsible Authority shall be required only to notify the User of this fact. The Responsible Authority shall not be obliged to notify the User whether it intends to report its findings to the police or will take any other measures. The provisions in Articles 11 and 12 shall apply mutatis mutandis. If the User is an Employee, the provisions in Article 13 shall apply mutatis mutandis.

Article 8 Reports and procedure to be followed

8.1 Reports concerning a User may only be made by letter or email. Each Report shall be supported by reasons and be clearly detailed.

8.2 Reports concerning students shall be made to the CGC, for which purpose the CGC has set up an email address, which is given on the ESA website. Reports that are made elsewhere within TU/e will be forwarded to the email address of the CGC. The Chairperson of the CGC shall assess the Reports.

8.3 Reports concerning Students are subject to the procedure set forth in Articles 9, 11 and 12.

8.4 Reports concerning Employees shall be made to the appropriate Managing Director.

8.5 Employees are subject to the procedure set forth in Article 13.

8.6 Reports concerning Third Parties shall (where applicable) also be made to the Responsible Authority of the Third Party concerned.

Article 9 Procedure following Reports concerning Students

9.1 Following a Report as referred to in Article 8.2, the Chairperson of the CGC shall ensure that the Student about whom the Report has been made is immediately identified.

9.2 Reports can be divided into the following categories:
- Manifestly or otherwise unfounded
- Misuse of a less serious nature, within the meaning of Annex 1.
- Misuse of a serious nature, within the meaning of Annex 1.

9.3 The Chairperson of the CGC may ask LIS to investigate the nature and scale of the use for which a Report concerning a Student has been received. LIS shall report as soon as possible to the Chairperson of the CGC on the findings of the investigation.

9.4 The Chairperson of the CGC shall decide:
- Whether the Report is manifestly or otherwise unfounded, or pertains to some form of Misuse.
- Whether the Report should be submitted to the full CGC in accordance with the provisions in Article 11.
- Whether the Report relates to fraud committed by one or more Students in relation to study units, or their components.

9.5 The Chairperson of the CGC shall inform the Responsible Authority for the Student in the event the Report relates to Misuse. The Chairperson of the CGC shall forward any Report concerning fraud in relation to study units to the examination board of the program being followed by the Student in question.

9.6 If the Chairperson of the CGC considers the Report to be manifestly or otherwise unfounded, he/she will deal with the Report himself/herself.

9.7 If the Chairperson of the CGC considers the Report to be well-founded and relating to Misuse of a less serious nature, he/she will deal with it as follows:
- If the Report is the first Report concerning a Student, the Student will receive a written warning from the Chairperson.
- If, within one year of the first Report relating to Misuse of a less serious nature, another Report about the same Student and relating to Misuse of a less serious nature is received, the Student concerned will receive a written notice of exclusion from the use of all ICT equipment and facilities. Possibilities exist for the Student to avoid that exclusion, however.

9.8 If, within one year after a temporary exclusion or after an exclusion has been lifted, a further case of Misuse by the same Student is reported, the Student will be summoned by the Chairperson of the CGC to attend a hearing to be questioned about the Report. In case of Misuse of a serious nature, the Chairperson will pass the Report on to the full CGC.

9.9 If the Chairperson of the CGC considers a Report relating to Misuse of a serious nature to be well-founded, the Report will be passed on to the full CGC for further handling. The Student to whom the Report relates will be notified of this in writing.

9.10 Where the Report gives reason to do so, including in cases of Misuse of a serious nature or

repeated or frequent Misuse of a less serious nature of the ICT equipment and facilities, the Chairperson of the CGC shall be authorized to take provisional measures against the Student with immediate effect, provided that the Chairperson of the CGC simultaneously notifies the Student in writing or by email of the decision in that regard, giving reasons for the decision. The measures may take the form of a warning or temporary exclusion from use of the ICT equipment and facilities, for example. Any provisional measure taken by the Chairperson of the CGC shall remain effective until the Responsible Authority, acting on the recommendation of the CGC and in accordance with the provisions of Articles 11 and 12, confirms, reverses or changes the decision to impose the measure. The Chairperson of the CGC shall not take any provisional measure until after consulting the Responsible Authority for the Student.

9.11 The Student may lodge an objection against the decision referred to in Article 9.10 with the Responsible Authority within six weeks of receiving that decision. The provisions in Articles 11, 12 and 14 shall apply mutatis mutandis. There is no possibility to lodge an objection against a practical measure which has no further legal consequences.

9.12 The decisions by the Responsible Authority pursuant to Article 9 can under no circumstances give rise to liability vis-a-vis the Student, the person who made a Report or any other person, unless in the event of willful misconduct or gross negligence attributable to the Responsible Authority.

Article 10 Special Persons

Electronic messages and information from the University Council and IGO members, members of the Faculty Councils and Service Department Councils, occupational physicians and other persons who have been given formal positions involving confidentiality by the Responsible Authority are excluded from any investigation or monitoring, except in cases where the provisions in Article 6 or Article 7 of these Regulations are applicable. This provision relates solely to electronic messages and information created, received and/or sent and/or stored by the aforementioned persons in the performance of their duties and where a direct relationship also exists with the performance of those duties.

Article 11 The Committee on Code of Conduct for Computer Use (CGC)

11.1 The CGC is tasked with investigating any Report made concerning a Student or a Report concerning a Student and issuing the Responsible Authority with advice in that regard concerning any measure to be taken against that Student.

11.2 The CGC consists of:

- The Chairperson of the CGC (ESA Director or mandatary appointed by him/her)
- The Secretary (LIS Director or a mandatary appointed by him/her)
- An Educational Director
- A lawyer
- A Student

The members of the CGC are appointed by the Responsible Authority for a term of four years, with the exception of the Student member, who is appointed for a term of one year.

11.3 The CGC is authorized to do everything it considers necessary to enable it to perform its duties and effectively carry out any investigation.

11.4 The CGC shall determine its own working methods, with due regard for the following:

a. The CGC shall only handle Reports which are submitted to in writing;
b. A report shall be made of the hearings of the Student;
c. The Student may be assisted by a counsellor at the hearing;
d. The CGC may, at its discretion, hear others. A report shall be made of any such hearing and, where possible, also be sent to the Student. The Student may attend the hearings of such others, unless the CGC unanimously decides otherwise;

e. All persons who are summoned by the CGC to attend a hearing are obliged to appear at the hearing and to provide any information that is requested;
f. CGC meetings at which Reports are considered are not open to others;
g. The CGC shall deliver written advice to the Responsible Authority, with a copy of the advice being sent to the Student. The advice may include measures to be taken by the Responsible Authority;
h. The CGC may seek the advice of experts;
i. The CGC shall issue its findings to the Responsible Authority in the form of a written report no later than six weeks after the hearing on a Report. The CGC's written report shall be accompanied by its advice concerning any measures to be taken.

11.5 The CGC shall prepare an annual report on its activities which shall be made public.

Article 12 Measures against Students

12.1 The Responsible Authority may, having regard to the advice and the report issued by the CGC, impose one or more of the following measures and/or sanctions against a Student who has acted in breach of the provisions in Article 2 and/or Article 4 as well as against any person whose user name, password and/or email address have been used in breach of Article 2 or Article 4:
a. A written warning, to which specific conditions may be attached;
b. The immediate removal or blocking of information. This may also include the removal or blocking of other information of the User. The Student shall be liable for any and all loss and/or damage resulting from the removal or blocking of information referred to in this Article, also including where other information than the Student's information is removed or blocked in the process;
c. Conditional or unconditional denial of access to and/or use of the ICT equipment and facilities, and/or use of the user name, password and/or email address, and/or conditional or unconditional denial of access to the TU/e buildings;
d. Reporting of a criminal offense;
e. If a third party makes a plausible case that his/her rights have been infringed, the identity of the Student may be disclosed to that third party, provided that such disclosure does not constitute any unauthorized or impermissible processing of personal data within the meaning of the General Data Protection Regulation.

12.2 A decision to deny a Student access may apply to all or part of the university buildings, grounds, ICT equipment and facilities. The TU/e Regulations and Guidelines for the Use and Management of Buildings shall apply mutatis mutandis.

12.3 A decision to impose measures as referred to in paragraph 1 above shall be made in writing by the Responsible Authority and shall be sent to the Student concerned by registered mail.

12.4 The Responsible Authority reserves the right at all times to deviate from the advice issued by the CGC. The Responsible Authority may also impose other measures than those stated in the advice.

12.5 The Responsible Authority shall make a decision within three weeks of receiving the advice of the CGC.

12.6 In urgent cases, the Responsible Authority may, by way of derogation from the provisions in this Article, impose measures as referred to in paragraph 1(a) to (d) with immediate effect. These measures will be notified to the Student concerned in writing and by registered mail.

12.7 The provisions in Article 11(4) shall apply mutatis mutandis to Users other than Employees or Students.

12.8 The CERT is authorized, in urgent cases or where necessary to avoid a risk, or the continued risk, of loss and/or damage, to take the necessary measures referred to in Article 7.5.

Article 13 Procedure and measures relating to Employees

13.1 In the case of employees of TU/e, non-compliance with these Regulations shall result in a disciplinary measure, as provided for under employment law.

13.2 The CERT is authorized, in urgent cases or where necessary to avoid a risk, or the continued risk, of loss and/or damage, to take the necessary measures referred to in Article 7.5.

Article 14 Use of social media

14.1 Use of social media is permitted with due regard for the provisions in Article 4.1 of these Regulations for matters relating to the position of the User concerned or the performance of his/her work-related duties. The User must, however, be careful not to harm the reputation of TU/e and the User. In other words: social media should be used responsibly.

14.2 TU/e supports open dialogue, the exchange of ideas and the sharing of the User's knowledge with others through social media. With respect to related topics, the User should ensure that the profile and content match how they would present themselves to others in text, image and sound.

14.3 Directors, managers, supervisors and others who promote policy or strategy on behalf of TU/e have a special responsibility when using social media, even where the content is not directly related to their work. Based on their position, they should consider whether, if applicable, they can publish in a personal capacity. They should be aware that others read what they write.

14.4 The sharing or dissemination of another person's personal data via social media in a professional capacity is only permitted if it is consistent with the employee's regular work activities and has been assessed for compliance with the GDPR. Particular attention should be paid to the dissemination of visual material (photos and videos) in which others can be identified; the express consent of the individuals concerned is usually required in this regard.

Article 15 Intellectual property and confidential information

15.1 This Article applies in particular to system administrators, for whom, in view of their special position, any breach of these provisions will be considered a serious dereliction of their duties.

15.2 The User shall treat any and all confidential information and privacy-sensitive information, including personal data, to which he/she has access in connection with his/her work or studies as strictly confidential and shall take adequate measures to ensure confidentiality in relation to such information.

15.3 The User may not infringe the intellectual property rights of TU/e and any third party, and shall respect the license agreements that apply within TU/e, as also referred to in Article 3.5 and Article 4.

15.4 Control of the institution's information lies with TU/e. The User has no independent control over the information, except where that has been explicitly granted by TU/e.

15.5 The User shall pay particular attention to implementing measures as referred to in these Regulations, if the performance of his/her work-related duties requires the processing of confidential information outside the institution (TU/e), including by email, in non-institutional cloud applications or on external storage media or personal devices (USB sticks, tablets, etc.). The User shall adhere strictly to any and all instructions and regulations drawn up by TU/e with regard to confidentiality, GDPR compliance and the protection of intellectual property.

Article 16 General Administrative Law Act (AWB)

In respect of the procedures referred to in these Regulations, the objection and appeal procedures under the General Administrative Law Act (Algemene Wet Bestuursrecht, AWB) are available only to Students after and to the extent that:

a) The procedure referred to in Article 11 of these Regulations has been followed;
b) A decision within the meaning of the General Administrative Law Act has been made.

Article 17 Applicable law

Dutch law shall apply in case of disputes arising from these Regulations or any other regulations or agreements. The competent court in the Netherlands shall have sole jurisdiction to hear disputes.

Article 18 Annexes

These Regulations have a single Annex, which may be amended by the full CGC. In case of amendment, the amended Annex shall be published on the TU/e website before it takes effect.

Article 19 Entry into effect

19.1 These Regulations may be cited as: the TU/e Regulations for Computer and Network Use.

19.2 These Regulations are effective from January 1st, 2023, and replace the Regulations which were adopted on January 1st, 2020.

Adopted by the Executive Board at its meeting of December 1st, 2022, after obtaining advice from the University Council.

Annex 1: Examples of classification of different types of misuse related to computer facilities

This listing gives examples of the application of the Regulations. The examples are provided for guidance purposes and are not exhaustive.

Misuse of a less serious nature (to be handled by the Chairperson of the CGC or the Managing Director)

Nuisance or disturbance caused by, for example:

- Games
- Sounds
- Chatting
- Screensavers and backgrounds
- Excessive running and use of hardware and peripherals
- Excessive network load

Misuse of a serious nature (to be handled by the CGC or the Managing Director), includes:

- Racist messages or posts
- Sexist messages or posts
- Insulting/abusive behavior
- Pornography
- Illegal copying
- Hacking
- Data manipulation
- Spreading of viruses and illegal software
- Sending email bombs/junk mail
- Causing intentional damage to hardware and peripherals
- By means of bots, script, etc., reading of files made available by the library which may only be accessed and/or used under license.