Leiden University Regulations on ICT and Internet Use

Version 1.0 – 4-11-2014

These Regulations state the rules regarding the use of ICT and internet facilities offered by Leiden University to its students, staff members, temporary personnel, visitors and others who have any type of agreement with Leiden University. These Regulations stipulate the responsible use of IT and internet facilities as well as the method of monitoring and inspection. These Regulations contain a balance between responsible and safe use of ICT and internet on the one hand and the privacy of the user on the other.

1. Definitions of terms

The terms in these Regulations are defined as follows:

Executive Board:	Executive Board of Leiden University
User:	anyone who uses the ICT or internet facilities made available by Leiden University, by means of an ICT workstation or any computer, laptop /notebook, PDA/smartphone, and such like, via remote access or otherwise. This group of users includes students, staff members, temporary personnel hired by the University, external academics and visitors;
ICT and Internet use/ provision of information:	any use, via remote access or otherwise, via the Network, SURFnet or via the ICT facilities offered by the University, including the provision of email;
ICT workstation:	a computer (PC, laptop/notebook, PDA/smartphone, and such like) which is owned by the University and operated by the User for ICT and Internet use.
Network:	the network of the University, both wired and wireless, which interconnects all the computer systems within the University, including those computers at home directly connected to the University or devices which staff members have received from the University to be used for work, which are connected to SURFnet and the internet;

Portfolio holder/Director:	portfolio holder of the operations of a University faculty or director of a support unit or facility of the University;
Regulations:	Regulations ICT and Internet Use Leiden University
Student:	anyone who is enrolled as a student at Leiden University and/or attends courses at the University;
SURFnet:	the national network infrastructure controlled by SURFnet, which interconnects the local networks of the institutions of higher education and research programmes, and to which the Network is connected;
Network Access configuration:	Settings of ICT workstations, servers and network equipment intended for identification of the system within the network as well as of the network traffic itself.
Network Access key:	the ULCN account or another combination of user name and password or other means of authentication (for example, using smartcards or tokens) which will give the user authorised access to the ICT and internet facilities of the University;
University:	Leiden University
Staff member:	a staff member as referred to in the Collective Agreement for Dutch universities, and employed by Leiden University.

2. Scope

2.1. These Regulations apply to the Users of the ICT and internet facilities as provided by the University, including email facilities.

3. General Conditions of ICT and Internet Use

3.1. The User is allowed to use the information facilities offered by the University only after having been granted permission by or on behalf of Leiden University; permission is granted through the provision of an account by the University.

3.2. The Access key issued to the User by the University is strictly personal and remains the property of the University. It is forbidden to give the Access key to a third party. The User is bound to strict confidentiality. Any person who has been issued with an Access key, must undertake or refrain from undertaking all those actions that can be reasonably expected of him to avoid misuse of his Access key.

3.3. The User is personally responsible for the use and subsequent use of his Access key.

3.4. The User must report any misuse, whether observed or suspected, through the usual channels immediately.

3.5. It is forbidden to secure the Access key belonging to other users and/or systems in any way or form.

3.6. The User must not access or try to gain access to those computer systems and/or data, for which no explicit access has been issued.

3.7. It is forbidden to change the access configuration of ICT workstations, servers or network devices belonging to the University.

3.8. The User may technically authorise a third party to gain access to his email facility (including his digital calendar). The third party uses his own Access key to access the other person's email and calendar.

3.9 The User is not allowed to copy or supply to third parties any software, data or records supplied by the University, unless permission (in writing) has been granted by the administrator.

3.10 The User must refrain from undertaking anything in his ICT and internet activities that may damage the reputation of the University, are unlawful or a criminal act. Any criminal act discovered by the University will be reported to the police.

3.11 The User who uses his own computer, laptop/notebook, smartphone and such like, for ICT and internet, is required to adequately protect this device or equipment against malware and, as far as is technically possible, install an adequate and up-to-date virus scanner and firewall.

3.12 The User is not allowed in any way to make accessible to the outside world any confidential information - according to the policy of information protection - or services on the University Network or internet, unless prior consent has been given by the Portfolio holder/Director.

3.13 The User is not allowed to connect network equipment (such as routers, servers and switches) to the network other than the equipment for which the administrator has granted permission.

3.14 The User must not impede or impose any disproportionate burden on the ICT infrastructure of the University when using the ICT and internet facilities.

3.15 The User is forbidden in any event to intentionally visit internet sites that contain pornography, including child pornography, racist or other discriminatory material, unless it is required to do so for free information gathering in the context of a study or research or professional duties and unless permission has been granted by the Portfolio holder/Director concerned.

3.16 The User is forbidden in any event to send or store any threatening, intimidating (including sexually intimidating), pornographic, racist or other discriminatory messages.

3.17 Email messages sent to and from the University are checked for malware. If necessary, infected messages will be removed or stripped of their malware.

3.18 The User must use an email account as supplied by the University when using the email facilities of the University. Communication on behalf of the University must take place via this account.

3.19 The User is not allowed to read, copy, change or delete email messages that are intended for others, unless explicit permission has been granted by the addressee or unless he is required to do so in the context of specific research as referred to in article 8.

3.20 The User is forbidden to use or exploit the provision of information for commercial ends.

4. ICT and Internet use - Staff member

4.1. The Staff member must use the ICT and internet facilities for professional duties.

4.2. The Staff member is allowed to use the ICT and internet facilities to a limited extent for private purposes, as long as this does not lead to an overloading of the ICT and internet system, or hinder him or others in their day-to-day work or offend others in any way.

4.3. In case of death, illness/incapacity for work, long-term absence or inadequate performance by the Staff member, the University has the right to allow the substitute or senior official to access the files or mailbox of the Staff member concerned. The substitute or Portfolio holder/Director is not allowed to access folders marked as private, email messages recognised as private, or email messages sent to or received from a confidential advisor, company doctor, or P&O staff member. If the Staff member has not marked any email messages as pri-

vate, the University may contact the staff confidential adviser to identify the email messages concerned as private and have them placed aside before allowing the substitute or senior official proper access. Email messages from members of the University Council, Faculty Boards, employee consultative bodies and other participation councils will not be examined, with due observance of the provisions set out in article 7 and 8.

4.4. Staff members who use the Network and SURFnet for internet access at home are not restricted in their private use at home. The private use of the Network and SURFnet at home falls exclusively under Dutch law. The other provisions in these Regulations apply in full to these Staff members.

5. ICT and Internet use - Students

5.1. Students must use the ICT and internet facilities for the benefit of their studies.

5.2. Students are allowed to use the ICT and internet facilities to a limited extent for private purposes, as long as this does not lead to an overloading of the ICT and internet system or offend others in any way.

5.3. Students who use the Network and SURFnet for internet access at home are not restricted in their private use at home. The private use of the Network and SURFnet at home falls exclusively under Dutch law. The other provisions in these Regulations apply in full to these Students.

6. ICT and internet use - temporary personnel, external academics, school pupils and visitors

6.1. Temporary personnel and external academics must use the ICT and internet facilities for carrying out their work for the benefit of the University. Visitors must use the ICT and internet facilities for the benefit of the reason for their visit to the University. School pupils must use the ICT and internet facilities for their application process.

6.2. Temporary personnel, external academics and visitors are allowed to use the ICT and internet facilities to a limited extent for private ends, as long as this does not lead to an overloading of the ICT and internet system, or hinder the temporary personnel or external academics or others in their day-to-day work, or offend others in any way.

6.3. In case of death, illness/incapacity for work, long-term absence or inadequate performance of temporary personnel, external academics and visitors, the University has the right to allow a senior official to access the files or mailbox of the person concerned. This Portfolio holder/Director is not allowed to access folders marked as private, email messages recognised as private, or email messages sent to or received from a confidential adviser, company doctor, or P&O staff member. If the person concerned has not marked any email messages as private, the University may contact the staff confidential advisor to identify the email messages concerned as private and have them placed aside before allowing the substitute or

senior official proper access. Email messages from members of the University Council, faculty boards, employee consultative boards and other participation councils will not be examined, with due observance of the provisions set out in article 7 and 8.

6.4. Visitors are only allowed access to the University information services at the location of the University libraries.

7. Monitoring and inspection

7.1. There is no systematic inspection of the content of the Network or ICT and internet use, other than is required for preventing malware and spam.

7.2. Electronic traffic and user information will be recorded and analysed regularly, in order to safeguard the optimal functioning of the ICT and internet facilities provided. This takes place in accordance with the current legislation regarding privacy and the protection of personal data.

7.3. ICT staff members are bound by a duty of strict confidentiality regarding ICT and internet data that can be traced back to individual persons.

7.4. The University fully adheres to the Data Protection Act and other relevant legislation when monitoring compliance with these Regulations.

8. Targeted investigation

8.1. Any User who is suspected of internet use which is contrary to these Regulations, he will be called to account by the Portfolio holder/Director as soon as possible.

8.2. A targeted investigation into a person will take place if misuse is suspected or asserted, as referred to in articles 3, 4, 5 and 6 of these Regulations.

8.3. A targeted investigation has the following main aims:

a. identifying misuse of ICT and internet facilities;

b. verifying existing agreements

c. verifying whether confidential information is adequately protected and has not been disclosed.

d. preventing negative publicity about the University.

8.4. The targeted investigation will take place on the written instruction of the Executive Board to the Portfolio holder/Director and will be carried out by an ICT officer specifically designated for this purpose. The instruction from the Executive Board will contain the reason for the investigation and the reason (if applicable) why the User was not notified by the Portfolio holder/Director prior to the investigation.

8.5. The Executive Board will be informed in writing about the results of the investigation. If the investigation findings give no reason for taking further measures, the written report will be destroyed.

8.6. Only if compelling reasons are found, a targeted investigation into the content of email messages and files will take place. These reasons are set out in the written instruction sent by the Executive Board.

8.7. Email messages and files belonging to University Council members, Faculty Board members, employee consultative board members, members of other partipation bodies, members of the degree programme committees, confidential advisers, trainee psychologists, company doctors and trainee counsellors are not excluded from the general monitoring and inspection of the system and network security. They are excluded from a targeted investigation as far as their email messages and files are concerned that are related to their performance as members of the participation body/degree programme committee.

8.8. A User who is to be the subject of a targeted investigation as referred to in article 8.4, will be informed in writing by the Executive Board as soon as possible about the reason, implementation and results of the investigation. The User will be given the opportunity to clarify the data in question. The obligation to provide information to the User will be disregarded if the provision of information in itself compromises the investigation. In that case the User will be informed about the investigation as soon as possible.

8.9 Items that should not be stored in ICT workstations or the Network, such as illegal software, films or music for private use, will be removed or legalised. The User will be informed about this beforehand by the Portfolio holder/Director concerned, unless this compromises the investigation.

9. Sanctions

9.1. If a Student acts in contravention of these Regulations, the Executive Board may impose the following sanctions:

a. temporary or otherwise restricted access to certain ICT facilities;

b. temporary or permanent ban on use of certain ICT facilities;

c. payment of costs resulting from the misuse in question;

d. temporary denial of access to the university buildings and sites;

e. termination of the Student's enrolment

9.2. If a Staff member acts in contravention of these Regulations, the Executive Board may impose the following sanctions:

a. temporary or otherwise restricted access to certain ICT facilities;

b. temporary or permanent ban on use of certain ICT facilities;

c. payment of costs resulting from the misuse in question;

other measures relating to a person's legal status including measures as referred to in the Regulation Disciplinary Measures Leiden University.

9.3. If another User acts in contravention of these Regulations, the Executive Board may impose the following sanctions:

a. temporary or otherwise restricted access to certain ICT facilities;

b. temporary or permanent ban on use of certain ICT facilities;

c. payment of costs resulting from the misuse in question;

d. temporary denial of access to the university buildings and sites;

e. termination of the User's contract with Leiden University

10. Liability

10.1. The University reserves the right to hold the User liable for all damage caused by the User as a result of his actions carried out in breach of these Regulations. These also include any damages claimed from the University by a third party as a result of the User's actions carried out in breach of these Regulations.

10.2. The University excludes all liability for any direct or indirect damages resulting from the use and (partial) disruption of the ICT and internet facilities of the University.

11. Final provision

11.1. In cases that are not provided for by these Regulations, the Executive Board will have the final decision.

11.2. These Regulations are valid from 1 February 2015 onwards and are referred to as the Leiden University Regulations on ICT and Internet Use. They replace the Code of Conduct for the use of ICT Facilities of 30 May 2005.