Regulations Usage of ICT-facilities and (personal) data by students of Leiden University of Applied Sciences

These regulations were adopted by the Executive Board of Leiden University of Applied Sciences on 14 October 2019, following approval by the Student Council on 8 October 2019.

Table of contents

Introduction

The processing of (personal) data and the usage of ICT-facilities (such as public computers, wireless and wired network connections, email and internet access, storage capacity, printers and electronic learning environments) are made available to the student for the purpose of study.

Leiden University of Applied Sciences, hereinafter referred to as 'the HSL', wishes to establish rules regarding the acceptable and desired usage of ICT-facilities and the usage of (personal) data. The aim is to strike a good balance between responsible, safe and workable usage of ICT-facilities and (personal) data and the privacy and security of its employees and students.

Nowadays, employees, students and the organisation also communicate with each other and third parties through social media and other (public) communication channels over which the HSL has no control. The rules of conduct in these regulations regarding the availability (continuity), integrity (reliability) and confidentiality (exclusivity) of data also apply to those channels insofar as the data relate to the HSL.

To gain insight into the technical usage of ICT-facilities and to be able to respond proactively to error messages, registration of use in log files is essential and important for optimising our ICT-facilities. In case of serious suspicion of violation of these regulations, logged (personal) data may be used in an investigation directed at a specific person. Those affected are to be properly informed about this. These regulations therefore also describe the manner and procedures for collecting student data, compliance monitoring and targeted investigation.

Leiden University of Applied Sciences is well organised and adheres to laws and regulations. In addition to the laws and regulations, this document is based on the Policy for Processing Personal Data, the House Rules and the Undesirable Behaviour Complaints Procedure Regulations.

Source reference:

These regulations for students at Leiden University of Applied Sciences are based on Model Regulations for Higher Education, a joint product of SURFnet and SURFibo.

Chapter 1 General provisions

Article 1 Definitions

- **Account**: HSL-account that is provided to each student upon (request for) registration;
- **Application**: computer programme or software, whether or not offered as a cloud service;
- **Management organisation**: is the term used for the officers authorised to manage ICT-facilities and to carry out logging, monitoring and possibly tracking. In practice, this will vary per implementation and may be assigned to functional management, technical management or a specifically designated officer within a faculty or service. The guideline describing the access policy is used to determine who is authorised for each application;
- **Primary business processes**: the activities of the HSL in the field of education and research;
- **Crisis**: a situation in which (a) the safety, health and/or welfare of students, staff and/or visitors of Leiden University of Applied Sciences is harmed, or (b) buildings, infrastructure or interests of Leiden University of Applied Sciences are damaged, or (c) the primary educational process is disrupted, or (d) strategic interests of the organisation are affected. In such cases, the existing normal hierarchical decision-making structure, procedures and protocols are not sufficient to control and combat the situation;
- **Data breach**: a personal data breach that poses a risk to the rights and freedoms of the person whose personal data are involved;
- **Diagnostic data**: recorded data of activities of users and systems and of events in ICT-facilities;
- **ICT-means of communication**: all means made available by the HSL to send messages to recipients inside and outside the HSL;
- **ICT-equipment**: hardware made available by the HSL, such as computers, laptops and network facilities. Private equipment is not included in this definition;
- **ICT-facility**: ICT-resources, applications and ICT-means of communication;
- **Logging**: the recording of activities or events of users and systems that take place in ICT-facilities and the storage of these records;
- **Monitoring**: the periodic checking and reviewing of diagnostic data for the presence of unwanted events and unusual situations such as violations of HSL-policies or threats affecting the availability, integrity or confidentiality of data or systems;

- **Personal data**: information about an identified or identifiable natural person as referred to in Article 4(1) of the General Data Protection Regulation;
- **Social media**: online platforms where users, with or without the intervention of editors, publish text and/or (audio-visual) images, exchange knowledge, opinions and experiences and enter into a dialogue with each other;
- **Confidential information**: information which the student knows or should know is confidential.

Article 2 Scope

2.1 These regulations set out rules with regard to the processing of (personal) data and the usage of ICT-facilities by students of Leiden University of Applied Sciences.

2.2 These regulations provide information on the way in which and the procedures in accordance with which automated data collection, the verification of compliance with these regulations and targeted investigation into individual students takes place.

2.3 For the purposes of these regulations, students of Leiden University of Applied Sciences include:

- Student or prospective student: the person registered as a student for a degree programme at Leiden University of Applied Sciences as referred to in section 7.32 of the WHW; in these regulations, a person who wishes to register as a student is also referred to as a student;
- External student: the person registered by the institution as an external student as referred to in sections 7.32 and 7.36 of the WHW for a full-time or part-time degree programme;
- Course participant: the person who is registered at Leiden University of Applied Sciences other than as a student or external student and who participates in education.

Article 3 Objectives

These regulations are intended to serve the following objectives:

- security of ICT-facilities, including protection against damage and misuse;
- preventing the ICT-facilities from being misused for sexual harassment, discrimination and other inappropriate behaviour;
- protection of the (personal) data of our employees, students and third parties;
- protection of confidential information of the HSL, its employees, students and third parties;
- protection of the intellectual property rights of the HSL and third parties;
- preventing the deliberate or accidental distribution of incorrect and/or non-current data and information;
- controlling availability, capacity and costs of the ICT-facilities of the HSL.

Article 4 Student rights

4.1 Information on students' rights in relation to the processing of their personal data by the HSL can be found in the Student Privacy Statement on the HSL-website.

4.2 Students can make a request regarding the processing of their personal data to the HSL-Data Protection Officer. Requests are handled in accordance with the procedure Handling of Requests regarding Rights of Data Subjects.

Chapter 2 Rules of usage and conduct for students

Article 5 (Personal) data and confidential information

5.1 If, in the context of their studies or the performance of tasks for the HSL, students gain access to confidential information and personal data, they must treat this information with strict confidentiality and take adequate measures (see also article 5.3) to ensure its confidentiality.

5.2 The student shall not infringe on the intellectual property rights of the HSL and third parties, and agrees to comply with the licensing conditions applicable to HSL-applications. This means, among other things, that students are forbidden to make educational materials (like syllabi, module manuals, presentations, (interim) examination questions, etc.) available to third parties, whether or not for a fee.

5.3 In the situation referred to in article 5.1, the student will take appropriate measures to prevent a data breach. Appropriate measures include in any case the following measures:

a. Confidential information and (personal) data are stored, saved and processed only within the systems of the HSL.
b. The processing of confidential information and (personal) data outside the HSL, such as sending information to external email addresses, the usage of cloud applications (e.g. Google-drive, WeTransfer, Dropbox) which are not under the control of the HSL, or the storage of data on external storage media or one's own equipment (USB sticks, external hard disks, tablets, etc.), is not permitted.

5.4 The student will strictly observe the rules set down by the HSL with regard to safeguarding confidentiality, including the rules in these regulations.

Article 6 Email and other ICT-means of communication

6.1 The HSL provides students with generic ICT-means of communication including internet access, an account, Office365 applications, an email system with associated email inbox and email address.

6.2 The following is prohibited in any usage of ICT-means of communication:

- sending or posting messages with a pornographic, racist, discriminatory, threatening, insulting, (sexually) intimidating or otherwise offensive content;
- sending or posting unsolicited messages to large numbers of recipients, sending chain letters or sending malicious software such as viruses, Trojan horses or spyware.

6.3 The student has sole access to his own HSL-email inbox. The only exception to this is described in Chapter 3 of these Regulations.

6.4 The following rules apply to the usage of email in the situation as referred to in Article 5.1:

a. The student shall not send emails containing confidential information or personal data, but shall use other more secure means of sharing such information, such as a personal interview.
b. Where possible, the student refers in the email to the (source) systems where the recipient can find the confidential information or personal data concerned. This prevents unnecessary copies of confidential information or personal data from entering the organisation and being retained.
c. If the options in sub a and b do not suffice, the student does not include the information in the email or in attachments, but shares a secure file containing the confidential information or personal data with the recipient.
d. The student always checks the link of the shared file and the email address of the addressee before sending the email. This prevents the wrong information from being accidentally shared with the wrong person.
e. The student uses bcc (blind carbon copy=hidden addresses) when addressing a group of external persons who may not have or need each other's data;
f. The student does not use the email application to store confidential information or personal data and therefore regularly deletes the relevant emails.

Article 7 ICT-equipment, applications and account

7.1 Computer and network facilities (ICT-equipment) are available to the student for study purposes. Limited private usage of ICT-equipment is permitted, provided it does not disrupt the good order or ICT-equipment of the HSL. Students should at all times be careful with the ICT-equipment provided.

7.2 The connection of personal equipment such as laptops, tablets and phones to the network is only permitted via the (wireless) network connections provided for this purpose. The Management Organisation may attach rules to the access to these connections in order to enforce these rules, such as having to install virus scanners and password protection. The connection of servers and network components (such as access points and routers) is not permitted without permission from the Management Organisation. Always contact the Service Desk for this.

7.3 The provisions in these regulations apply in full to students who use an HSL-network facility in their accommodation. No additional restrictions are imposed on the usage, except as may be necessary to preserve the integrity and security of the network, or to ensure (the speed of) network traffic. If the Management Organisation intervenes, similar types of network traffic will be treated equally.

7.4 The storage of private files or information on the personal storage location of the HSL is permitted, provided it does not lead to an overload of the ICT-facilities or disrupt the good order in the workplace. Furthermore, the content of the files and information must not violate any laws or regulations.
The HSL is not obliged to make back-up copies of such files or information or to make copies available. Usage of the personal storage location of the HSL for private use is at your own risk.

7.5 The HSL may prescribe systems or applications for educational processes, such as a Digital Learning and Working Environment (DLWO, *Digitale Leer- en Werkomgeving*), an email system, (mobile) applications, apps, cloud facilities, or multimedia services. The faculty or degree programme may set additional conditions for the use of systems or applications.

7.6 The independent installation of software on the computer and network facilities of the HSL is not permitted if the Management Organisation has set restrictions that prevent installation.

7.7 The circumvention of security facilities at ICT-facilities of the HSL is not permitted.

7.8 At all times, students must treat their personal HSL account, log-in details and any additional means of authentication (such as One-Time-Passwords or SMS authentication) with care. Personal passwords and additional means of authentication may not be shared.

7.9 The usage of ICT-equipment by the student for commercial activities is only permitted with the written permission of the HSL.

Article 8 Internet

8.1 Access to the Internet and related facilities will be provided to the student for the purpose of studying. Limited private usage of internet is permitted,

provided that it does not interfere with the good order at the HSL or the ICT-equipment of the HSL.

8.2 However, the following activities are prohibited during all internet usage:

- visiting sites that contain pornographic, racist, discriminatory, insulting or offensive material;
- the use of file sharing or streaming services if this generates excessive data traffic, to the extent that it may jeopardise the availability of the ICT-facilities;
- downloading films, music, software and other copyrighted material from any illegal source or when the student actually knows that this is in violation of copyright;
- distributing (uploading) films, music, software and other copyrighted material to third parties without the consent of the rightsholders.

Chapter 3 ICT-management measures and control

Article 10 General provisions

10.1 The Management Organisation will only gain access to a student's account or ICT-equipment with the student's consent. Access without this permission is only permitted in exceptional cases and according to the procedures as described in this chapter.

10.2 The automated collection of data about, control of and targeted investigation into usage of the ICT-facilities and internet usage will only take place in the context of enforcing the rules of these regulations for the purposes referred to in article 3. Prohibited or undesired usage is made impossible by technical means as much as possible.

Article 11 Recording of ICT-, email and internet usage (logging)

11.1 For the purpose of proper and efficient management of the ICT-facilities of the HSL, data are collected (logged) automatically whenever possible, including:

- date, time
- username/identification
- workstation/location information
- activity/event
- the device on which the activity was carried out
- if relevant, the result of the activity

11.2 These logged data are accessible to the Management Organisation. The logged data shall only be made available to other officers on the basis of the guideline that defines the access policy.

11.3 The logged data will be kept for a maximum of 6 months and then destroyed. In the case of incidents, logged data is kept as long as necessary to handle the incident + 1 year to perform any monitoring or corrective analysis.

Article 12 Monitoring ICT-, email and internet usage (monitoring)

12.1 Monitoring means periodically checking and assessing diagnostic data for the presence of unwanted events and unusual situations such as violations of HSL-policies or threats affecting the availability, integrity or confidentiality of data or systems. The result of the assessment is converted into an alert for the Management Organisation and possibly into a report to relevant officers.

12.2 In response to an alert, the Management Organisation can take preventive measures within the ICT-facilities to eliminate the threats.

12.3 In the event of suspected misuse of a password, account and/or login data, the HSL has the option of disabling access to the relevant account with immediate effect.

12.4 Based on the results of the monitoring, a targeted investigation into compliance with the rules of these Regulations as referred to in article 13.1 may be started.

Article 13 Targeted investigation into violation of these regulations

13.1 A targeted investigation occurs when diagnostic data or personal data concerning a specific student are recorded within the framework of an investigation following a serious suspicion of a violation of these Regulations by that student.

13.2 Targeted investigation by the Management Organisation will only take place after written instructions from the Faculty Director under whose responsibility the student falls. The Executive Board shall receive a copy of these instructions and the written results of the investigation. If the investigation does not give rise to any further measures, the instructions and the results will be immediately destroyed by the Management Organisation.

13.3 Targeted investigation is initially limited to diagnostic data of the usage of ICT-facilities. If targeted investigation provides further evidence of violation of these regulations, the Management Organisation may, with the consent of the instructing director as referred to in 13.2 and the Executive Board, proceed to inspect the content of messages or stored files if this is necessary for the investigation. Only data clearly marked as 'confidential' will be treated by the HSL as such.

13.4 The student will be informed in writing as soon as possible by the director of his faculty about the reason for, the execution of, and the result of the investigation. The student is given the opportunity to give an explanation about the data found (hearing both sides). Postponing notification is only allowed if notification would actually harm the investigation.

13.5 A targeted investigation is carried out in accordance with the multiple-eyes principle. This means that it always involves multiple people.

Article 14 Measures in case of other special situations

14.1 In addition to the measures mentioned in this chapter relating to management, control and targeted investigation, the Management Organisation will only gain access to a student's account or ICT-equipment in the following special situation and in accordance with the procedure described in this article.

14.2 In the event of a possible crisis, the Executive Board or the crisis team may grant permission to the Management Organisation to gain access to the account (such as emails and files) of one or more students, if this is necessary to safeguard the continuity and quality of the primary business processes of the HSL. Confidential files are not read if they are labelled as such.

14.3 The student will be informed in writing as soon as possible by the director of his faculty of the measures that have been or will be taken on the basis of this chapter.

14.4 The implementation of measures in special situations is always based on the multiple-eyes principle when carrying out the investigation. This means that it always involves multiple people.

Chapter 4 Violation of these Regulations

Article 15 Consequences of violation

In the event of a breach of these Regulations or of generally applicable legal rules, the Executive Board and/or the director responsible may, depending on the nature and seriousness of the breach, take appropriate measures.

Chapter 5 Final provisions

Article 16 Final provisions

16.1 These Regulations shall be evaluated every two years under the direction of the Information Management Department and revised where necessary.

16.2 These Regulations may be amended in the interim with the consent of the Student Council, if circumstances so require. Proposed changes are announced to the students and Student Council prior to implementation.

16.3 In cases not covered by these Regulations, the Executive Board shall decide.