



Regulations on ICT Facilities and Personal Data

Section 1. General Provisions

Article 1.1 Definitions

In these Regulations, the following definitions apply:

1. Account: The right of access to ICT facilities;
2. Data subject: A person whom an item of personal data relates to, or a person who uses the ICT facilities which are referred to in these Regulations and which Hanze University makes available;
3. Hanze University: Hanze University Groningen;
4. ICT facilities: All the information and communication facilities made available by Hanze University including any infrastructure, network facilities, peripheral equipment, email, Blackboard and the Internet;
5. Staff: Any natural person who is on work placement at Hanze University or is employed by Hanze University to carry out work, regardless of the nature or scope of their employment;
6. Personal data: Any information relating to an identified or identifiable natural person;
7. Phishing: An email message intended to gain access to an account or password;
8. Spam: Unsolicited email sent in bulk;
9. Student: A natural person who is registered at Hanze University for the purpose of receiving education and/or taking examinations, or who was previously registered at Hanze University as a student;
10. Processing of personal data: Any operation or set of operations relating to personal data including the collection, recording, organising, storage, processing, modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging or linking of personal data, as well as the blocking, erasure or destruction of such data.

Article 1.2 Scope

1. These Regulations apply to the use of accounts and ICT facilities which are made available by Hanze University to its students and staff.
2. These Regulations also apply to all the processing of personal data within Hanze University which relates to the University's staff or students.

Article 1.3 Objectives

1. The objectives of these Regulations are:
 - a. to limit the use of the facilities made available by Hanze University that is not related to study or work;
 - b. to protect and secure Hanze University's systems and information.
2. These Regulations also aim to:
 - a. protect the privacy of the data subjects whose personal data are processed against misuse of these data and against storage of inaccurate data;
 - b. prevent personal data which are processed from being used for a purpose other than that which they are intended to be used for.

Article 1.4 Data Control and Records Management

1. The Executive Board of Hanze University is the Data Controller responsible for the processing of all data including personal data.
2. The Head of the Student Administration is the Records Manager responsible for the processing of personal data relating to students.
3. The Head of the Personnel and Organisation Staff Office is the Records Manager responsible for the processing of personal data relating to staff.



Section 2. Use of Accounts and ICT Facilities

Article 2.1 Accounts

1. Individual accounts are made available by Hanze University to its staff members and students for the duration of their employment or enrolment, respectively.
2. The data subject must ensure that their login code and password can only be used by themselves. They must take appropriate measures to keep their password secret.
3. The data subject must take security measures with respect to the equipment which they use to log in to Hanze University facilities from outside the University, in order to prevent any unauthorised use of the University's ICT facilities and/or information.

Article 2.2.1 ICT Facilities

1. ICT facilities may not be used for commercial purposes.
2. Use of ICT facilities which is not related to study or work is allowed unless it conflicts with the interests of Hanze University.
3. ICT facilities may not be used for sending or posting messages or documents which have sexually harassing, pornographic, discriminatory, racist, insulting, defamatory or offensive content.
4. Hanze University may lay down further rules regarding the use of specific ICT facilities including notebooks and tokens. These rules may require the data subject to sign a statement of confidentiality for the processing of certain data.
5. Adding or disconnecting equipment including hubs, routers, bridges and switches to/from the infrastructure is not allowed.

Article 2.2.2 ICT Facilities: Email

1. Email addresses are made available by Hanze University to its staff and students for the duration of their (employment) contract or their enrolment, respectively.
2. Email messages must be signed by the data subject using their own name.
3. Email messages may not incite hatred or violence. The use of ICT facilities for chain letters in whatever form or for whatever purpose, is not permitted, nor may ICT facilities be used for phishing or spamming.
4. Without the Dean's permission, no messages may be sent to all the students and/or staff of a school.
5. It is not permitted to send messages to all the staff members of a Staff Office or Unit without the permission of the Director of the Staff Office or Unit concerned.
6. Without permission from the Marketing and Communication Director, it is not permitted to send messages to all the staff or students of Hanze University.
7. The data subject must ensure that information which is sent by email and which the data subject regards as confidential, or which they ought to suspect is confidential, is kept confidential.
8. Email archives are managed by the data subject themselves on the understanding that Hanze University may limit the size of individual archives. The data subject must reduce the size of their archive if the limit is exceeded.

Article 2.2.3 ICT Facilities: the Internet

1. The Internet must not be used for visiting websites which have pornographic content or websites which the data subject should understand it would harm the honour and reputation of Hanze University to gain access to their content.
2. Similarly, the Internet must not be used for the uploading or downloading of files, whether intentionally or accidentally, which have content that the data subject should understand it would harm the honour and reputation of Hanze University to gain access to them.

Article 2.3 Access to the Account and Email Archive in the event of Long-Term Absence

If continuity of work necessitates this, the Executive Board may grant access to the account and email archive of a staff member who is absent for a long period of time because of illness or leave, or who has left the service of Hanze University or who has died, to a user designated by the Executive Board for a



limited period of time. The staff member or their surviving relatives will be notified accordingly in writing.

Article 2.4 Blocking and Inspecting Accounts and Email Archives in the event of Misuse or Suspension

1. If there is good reason to suspect that a staff member has been misusing ICT facilities, the Executive Board may decide to block their access to these facilities. The staff member will be notified of this in writing.
2. The Executive Board may also decide to block a staff member's access to ICT facilities if they have been suspended from work, for the duration of the suspension. The Board will notify the staff member accordingly in writing, stating the reasons.
3. If there is good reason to suspect that a student has been misusing ICT facilities, the Dean may decide to block their access to these facilities. The Dean will notify the student accordingly in writing, stating the reasons.
4. If a decision of the kind referred to in the second and third paragraphs is taken, safeguards will be provided so that the data subject will continue to have the opportunity to refer to information about legal remedies as well as any other information which should reasonably be available to them.
5. If there is good reason to suspect that a staff member or student has been misusing ICT facilities, the Executive Board may decide, for the purposes of an investigation, to gain access to that person's account in order to inspect the information, documents and email archive contained within it.

Section 3. Processing of Personal Data

Article 3.1 Processing of Personal Data

1. For the purposes of privacy protection, the Executive Board will ensure that personal data of students or staff which are processed are protected against misuse, and will prevent any personal data from being used for purposes other than what it is intended for, in accordance with the relevant provisions of the Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*).
2. The data processing operations carried out by Hanze University only involve personal data that have been obtained lawfully and are in accordance with the purposes which the processing system was installed for.
3. The Executive Board will make the necessary provisions to promote the accuracy and completeness of the personal data recorded in Hanze University's systems. The Board will also provide the technical and organisational facilities which are necessary to protect the processing of personal data against loss or mutilation of the data and against their unauthorised disclosure, modification or removal.
4. Hanze University only discloses information to third parties if it is inherent in the purpose of the processing, or if it is required pursuant to statutory provisions, or if the data subject gives his/her permission. On request, data may be disclosed anonymously to persons or administrative bodies with public law duties but only if they need the data for the execution of their duties and this does not infringe the privacy of the data subject.

Article 3.2 Organisation and Management of Processing Systems

To guarantee the proper organisation and management of processing systems, the Executive Board keeps a written register. This register must at a minimum contain the following information about Hanze University's systems for processing personal data:

- a. insofar as it is required, the notification to the Dutch Data Protection Authority (the *College Bescherming Persoonsgegevens*);
- b. the purpose and the process involved;
- c. the category of persons concerned;
- d. the type of data;
- e. provision of information to third parties;
- f. retention periods;
- g. connections to other processing systems;



- h. authorised officers;
- i. the functional and technical Systems Manager.

Article 3.3 Right of Access

1. The data subject has the right of access to their personal data, which must be presented in a comprehensible form, and to learn the source of the information about them that is contained in the processing systems, and to what third parties the information has been disclosed.
2. To gain access to their personal data, the student must make a request to the Student Administration. Staff must make requests to the P&O Director. The decision about a request will be notified as soon as possible, but no later than four weeks after the request was made. A refusal to comply with a request must state the reason(s) why.

Article 3.4 Right to rectification, destruction and blocking

1. If a data subject can prove that certain information relating to them is inaccurate or incomplete, or is irrelevant for the processing purposes or is in conflict with a legal provision or these Regulations, they are entitled to have those data rectified, supplemented or removed.
2. Students must make requests for this purpose to the Student Administration. Staff must make their requests to the P&O Director. The request must state what changes should be made. The decision about the request will be notified to the data subject as soon as possible, but no later than within four weeks. A refusal to comply with a request must state the reason(s) why.

Section 4. Further Provisions

Article 4.1 Sanctions

1. If a student violates any of the provisions of these Regulations, the Dean may take the disciplinary measures referred to in the Disciplinary Rules of Hanze University; these are included in Appendix 10 of the Student Charter.
2. If a staff member violates any of the provisions of these Regulations, the Executive Board may take the disciplinary measures referred to in Section P of the Collective Labour Agreement for Higher Professional Education (CAO-HBO).

Article 4.2.1 Legal Protection of Students

1. Objections against the decisions referred to in Article 3.3, second paragraph and Article 3.4, second paragraph, must be lodged with the Head of the Student Administration. The time limit for lodging objections is four weeks counting from the date that the decision was sent. Objections are decided upon within six weeks.
2. Objections against the decisions referred to in Article 2.4, third paragraph and Article 4.1, first paragraph, must be lodged with the Student Appeals Board, as referred to in Chapter 11 of the Student Charter.

Article 4.2.2 Legal Protection of Staff

1. The decisions referred to in Article 2.4, first paragraph, Article 3.3, second paragraph and Article 3.4, second paragraph, are subject to legal remedy, as referred to in the General Rules regarding Staff Appeals and Objections (*Algemene regeling voor beroep en bezwaar van het personeel*).
2. The procedure referred to in Section P of the Collective Labour Agreement for Higher Professional Education (CAO-HBO) applies to the decisions referred to in Article 2.

Article 4.3 Publication

These Regulations will be included in the Student Charter as an Appendix. They will also be published on Blackboard.

Article 4.4 Entry into Force

These Regulations will enter into force on the day after they have been adopted by the Executive Board with the approval of the Hanzehogeschool Participation Council.



Hanze University Groningen
APPLIED SCIENCES

Adopted by the Executive Board on 25 May 2009.

This document is a translation. In the event of any dispute as to the interpretation of any of the provisions set out in this document, the official version in Dutch will prevail.