Acceptable Use Policy HZ students

Regulations for ICT and internet use for students of the HZ University of Applied Sciences

Acceptable Use Policy for students of the HZ University of Applied Sciences

The HZ University of Applied Sciences (hereinafter the Institution) offers its own and visiting students the opportunity to use the internet for the benefit of their studies. Additionally, students are offered an institutional mailbox for personal use as well as the possibility of saving files and personal study data for the purpose of studies. Certain rules apply to the use of these facilities, in the context of the smooth running of things in the Institution's buildings and grounds.

Use of facilities

Computer and network 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 purposes of the study, such as making assignments, reports and theses, logging the study progress, consulting sources, and communicating with teachers and fellow students.
The use of one's own equipment and applications on the facilities of the Institution is permitted as long as this use complies with the rules of these Regulations. Changing settings in equipment and applications made available by the Institution is only allowed with the separate permission of the administrators. Connecting one's own network equipment which allows the connection to be shared with any third party on the wired or wireless network connections is prohibited at all times.

These Regulations also apply if you are a guest user of network facilities of another institution where access is granted with the login credentials of one's own Institution (Eduroam).

Certain facilities can only be accessed with a user name and password. These are strictly personal and may not be shared with others. The system administrator can pose additional demands for the quality of passwords and other security aspects, as further set out in the information security policy. In the case of suspected misuse of a password, the system administrator can immediately suspend access to the account in question.

Intellectual property and confidential information

The student does not breach the intellectual property rights of the Institution and third parties and respects the license agreements as applicable within the Institution.
The control over the Institution's information rests with the Institution. The student has no independent control over the information unless this is explicitly granted by the Institution.

If the student gains access to confidential information or privacy-sensitive information during the course of his studies or while carrying out tasks for the Institution, the student must treat this information as strictly confidential.
The student pays particular attention to the measures as listed in these Regulations, if the performance of the work requires processing of confidential information outside the Institution, such as via email, in non-Institutional Cloud applications, on external storage media or private client devices (USB devices, Tablets, etc.).

If the Institution has drawn up rules with regards to ensuring confidentiality and the intellectual property rights, the student must strictly comply with these.

Security by the Institution and the student

The Institution takes information security seriously. As such, it adopts a strict security policy and takes appropriate technical and organisational measures to protect its infrastructure against loss, theft, criminal activities, loss of confidentiality, invasion of privacy rights and infringement of intellectual property.
Perfect security is of course impossible. Therefore, the institution expects students to adopt a proactive attitude and undertake serious steps in order to adequately secure their own computers and other equipment (such as smartphones or tablets). The student is thus at all times responsible for the use of his own equipment and the data saved on this equipment.

In particular, the student must do the following in the context of security if using the Institution's facilities with his own equipment:

- install an adequate virus scanner and firewall;
- make regular backups of all relevant data and safely store copies of Institutional data;
- use strong passwords;
- keep this equipment up to date in terms of software settings;

Private use and disturbance

Limited private use of the facilities is allowed. Use, either private or for the purposes of study, should not disturb the smooth running of the Institution and should not cause disturbance to others, infringe Institution or third-party rights or compromise the integrity and security of the network.

Use which causes disruption or disturbance is in any case defined as:

- consulting internet services with a pornographic, racist, discriminatory, offensive or objectionable content in public areas or sending messages with such content;
- sending messages with (sexually) intimidating content or messages that (can) incite discrimination, hatred and/or violence;
- sending messages to large numbers of recipients at a time, sending chain letters or distributing malicious software such as viruses, Trojan horses and spyware;
- using file sharing or streaming services if this generates too much data traffic, in such a way that it could endanger the availability of the facilities;
- downloading films, music, software or any other copyrighted material from any illegal source, or if the student knows or should know that this constitutes a breach of copyright;
- distributing (uploading) films, music, software and other copyrighted material to third parties without the permission of the copyright holders.

It is not allowed to use the HZ network for engaging in activities which are illegal according to the criminal code.

The use of computer and network facilities for commercial activities is permitted only if the Institution has granted written permission for this.

Monitoring by the Institution

Checks of facility use only takes place within the framework of enforcing the rules in these Regulations for the benefit of the smooth running of the Institution and the safeguarding of the integrity and security of the Institution's network and computer facilities.

Prohibited use of the facilities is made prevented by technical means as much as possible. Data is automatically collected (logged) for these checks. This data

is only accessible to the directly responsible employees of the Information and Automation Department, and is only made available to other administrators and authorised parties anonymously. These can decide to take further technical measures, such as blocking access to a particular service or limiting the capabilities of the device in question in being able to use the network.

In particular, in the case of disturbance caused by student equipment, the network access possibilities may be shut down. If possible, students are warned in advance, so that they have the opportunity to halt the disturbance. If this - due to urgency - is not possible prior to taking the measure, the measure is reported as quickly as possible.

In the case of suspected violation of the rules, checks can be carried out at the level of individual data traffic of the email and use of the facilities. Only in severe cases do checks on content take place.

The Institution fully complies with the personal data protection act and other relevant laws and regulations when carrying out checks at the level of traffic data or content. In particular, the Institution secures the data recorded for checks against unauthorised access and persons with access to this are contractually bound to confidentiality.

Procedure for targeted investigation

Targeted investigation is undertaken when traffic data or other personal data relating to a specific student is recorded in the context of an investigation in response to a serious suspicion of a breach of these Regulations by that student.
Targeted investigation only takes place following a written command from the director of the faculty, mentioning the reasons why it is being carried out.
The Executive Board will receive a copy of this command and a record of the results of the investigation.

Targeted investigation is initially limited to traffic data from the use of the facilities. If targeted investigation provides further evidence, the Institution following separate permission may proceed to an examination of the content of communications or stored files. If the investigation does not give rise to further measures, the records will be destroyed.

Targeted investigation of the security or integrity of peripherals may, in deviation from this, be carried out by the system administrators on the basis of concrete indications without separate permission. The results of this investigation are only shared with the student for the purpose of enhancing the security or integrity of peripherals. In case of repetition, the procedure in the previous clause will be followed.

The student is informed in writing by or on behalf of the Executive Board about the cause, the execution and the result of the investigation as soon as possible. The student is given the opportunity to provide an explanation about the retrieved data. Postponement of this notice is only allowed if it would actually impair the investigation.

System administrators only gain access to accounts or computers of students if the student has given his permission for this. Access without this consent is only allowed in urgent cases or in the case of a clear presumption of violation of these Regulations, as specified in this article. The student will in that case be informed afterwards.

Rights of the student with regards to personal data

The student may submit a request to the Board for a complete overview of his personal data as processed by the Institution in the framework of these Regulations. A response to such a request is given within four weeks.

The student can ask the Board to improve, to complete, to delete or to shield his personal data, if these are factually inaccurate, incompletele or irrelevant for the purpose, or in violation of any law. A response to such a request is provided within four weeks. A refusal is explained with reasons. An approved request will be carried out as quickly as possible.

The student may also further oppose processing of his personal data in connection with serious personal circumstances. The Board will decide whether this objection is justified within four weeks of receipt. If the Board deems the objection to be justified, it will immediately terminate the processing.

Consequences of violation

When acting in violation of these Regulations or the generally applicable legal rules, the Institution board can take disciplinary measures depending on the nature and severity of the violation.
These include a warning, a reprimand, a temporary closure or restriction of facilities (up to one year) and in extreme cases a termination of registration as a student.

Disciplinary action (except a warning) cannot be taken solely on the basis of an automated processing of personal data, such as the discovery of an automatic filter or lock. Furthermore, no disciplinary measures are taken without giving the student the opportunity to defend his point of view.

In deviation from the above, the Institution may upon (automated) discovery of a disturbance implement a temporary block of the facility in question.
The block will be maintained for a week at most, or for a shorter period if the system administrator deems the cause to have been removed satisfactorily. If no improvement has been observed by the system administrators within a week, the system administrators can decide to implement a longer block. Upon repeat incidents of the cause, disciplinary measures may be taken.

Final provisions

These Regulations may be revised by the board. Changes are only implemented at the beginning of an academic year, except in urgent cases or if the Institution is forced to implement these more quickly due to outside circumstances.

Changes are only implemented after a prior recommendation has been requested from the Institution participation council. The Board will take feedback from students into consideration before implementing the changes.

In any circumstances not provided for in these Regulations, the Executive Board’s decision shall be final.