Acceptable Use Policy HZ employees

Rules for ICT and internet use for employees of the HZ University of Applied Sciences

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

Basis for the regulations

For (many) HZ employees, the use of the internet and ICT resources is necessary in order to be able to perform their job properly. However, there are risks related to this use which require establishing rules of conduct. Against the background of these risks, the employees are expected to make responsible use of the internet and ICT.

With these Regulations, the institution, HZ University of Applied Sciences, hereinafter referred to as "the Institution" wishes to set rules with regards to the desired use of operating assets. The aim here is to strike a good balance between responsible and safe ICT and internet use and the privacy of the employee.

The use of social media such as Facebook, LinkedIn and Twitter is becoming increasingly important but can also affect the Institution. Therefore, the Institution would like to lay down certain rules for this as well.

The Institution is as an employer authorised to impose rules regarding the performance of the work and the good order of the workplace, as determined by law. These Regulations are in addition to the law also based on the CAO HBO.

Article 1. Principles

1.1. The Regulations lay down rules regarding the professional use of ICT and internet by employees. The goal of these regulations is to determine good order with regards to

- system and network security, including protection against damage and misuse;
- prevention of sexual harassment, discrimination and other criminal offences;
- protection of sensitive and personal information including personal data of the Institution and its employees, and that of students and parents;
- protection of confidential information of the Institution and its employees, and that of students and parents;
- protection of the intellectual property rights of the institution and third parties including the respect for the licensing agreements that apply within the institution;
- prevention of negative publicity;
- cost and capacity management.

1.2. Limited private use of internet and ICT tools is only allowed during breaks and/or insofar as the work does not suffer. Use for ancillary activities is prohibited at all times unless separate written consent has been obtained.

1.3. These Regulations apply to all those working for the Institution, including temporary workers. These Regulations do not apply to (guest) students; separate Student Regulations have been drafted for this.

1.4. 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 the own Institution (Eduroam).

1.5. In the framework of enforcing these Regulations, the Institution strives towards measures that limit access to sensitive information or the personal data of individual employees as much as possible. Where possible, the Institution will only carry out automated checks or filters, without allowing other people or itself insight into the behaviour of individual persons.

Article 2. Intellectual property and confidential information

2.1. The employee should treat confidential information, privacy-sensitive information including personal data to which he has access in the work context, with strict confidentiality and take sufficient measures to ensure confidentiality.

2.2. The employee does not breach the intellectual property rights of the Institution and third parties and respects the license agreements as applicable within the Institution.

2.3. The control of the Institution's information rests with the Institution. The employee has no independent control over the information unless this is explicitly granted by the institution.

2.4. The employee pays particular attention to the measures as listed in these Regulations, if the performance of the work requires processing of sensitive information outside the Institution, such as via E-mail, in non-Institutional Cloud applications, on external storage media or private client devices (USB devices, Tablets, etc.).
If the Institution has drawn up regulations with regards to ensuring the confidentiality and protection of intellectual property, the employee will strictly comply with these.

2.5. These provisions apply in particular to employees of the Information and Automation Department, for whom violation of these provisions is considered a very serious breach of duty, given their special position.

Article 3. Use of computer and network facilities

3.1. Computer and network facilities are made available to the employee for use in the context of his function. Use is therefore bound to tasks arising from this function. Private use of these resources is permitted only as provided for in article 1.2.

3.2. The employee should at all times make careful use of the login credentials and any other means of authentication (such as smartcards and tokes) provided to him. Personal passwords and additional authentication methods may not be shared. In the case of suspected misuse of a password, the system administrator can immediately suspend access to the account in question.

3.3. The Institution can prescribe systems or applications for education and other business purposes, such as an Electronic Learning Environment, an email system, (Mobile) Applications (Apps), Cloud facilities or multimedia services. The employee will, for sharing teaching materials or conducting research, only use these systems and agree to abide by the applicable limitations and requirements.

3.4. Connecting servers and active network components (such as access points and routers) are not allowed without the authorisation of the Information and Automation Department. The service can attach rules to the authorisation in the framework of enforcing these regulations, such has having to install virus scanners and password security.

3.5. Connecting private client equipment (such as, laptops, tablets, and phones) is only permitted on the (wireless) network connections provided for this. The Information and Automation Department can attach rules to this access in the framework of enforcing these regulations, such has having to install virus scanners and password security.

3.6. Saving private files or information on Institution systems is permitted, provided that this does not overload the storage capacity of these systems or cause a disturbance of the good order on the work floor. The Institution is however not required to make backups of such files and information, or to make copies available in the case of replacement or repairs of the systems in question.

3.7. The use of computer and network facilities by the employee for ancillary activities is permitted only if and insofar as the Institution has granted written permission for this.

Article 4. Use of email and other ICT communication tools

4.1. The email system and the corresponding mailbox and email address are made available to the employee for use in the context of his function. Use is therefore bound to tasks arising from this function.

4.2. Private use of these resources is permitted only as provided for in article 1.2.

4.3. However, the following is prohibited during any use (private or not) of ICT communication tools:

- sending messages with pornographic, racist, discriminatory, threatening, insulting or offensive content;
- sending messages with (sexually) intimidating content;
- sending messages that (can) incite discrimination, hatred and/or violence;
- sending unsolicited messages to large numbers of recipients, sending chain letters or malicious software such as viruses, Trojans or spyware.

4.4. The employee will preferably not use the email address provided by the Institution for private emails, within the limitations of article 1.2. The organisation will not block or specifically monitor the access to other email services.

4.5. In case of illness, unexpected long-term absence or gross negligence on the part of the employee, but only if this constitutes a serious reason of corporate interest for access, the Institution is entitled to give a replacement or superior access to the files or the employee's mailbox, but only after separate permission from the Executive Board has been obtained. It should not, however, provide access to folders marked as private, recognizably private emails, or emails sent to or from a confidant/company doctor/HR Officer. If the employee has not placed such markings, the Institution can check the relevant information of the employee with the help of a confidant in order to designate private information and separate it before giving the replacement or superior access.

4.6. Email messages from members of the representative body to each other, from company doctors, HR consultants and anyone who can lawfully appeal to confidentiality, are not checked. This does not apply to automated security checks of the email traffic and network.

4.7. The employee agrees to the automatic placement by Institution applications of copies of messages which were recorded using these applications in the email box and agenda of the employees in the Institution's email system.

Article 5 Use of internet

5.1. Internet access and the related facilities are made available to the employee for use in the context of his function. Use is therefore bound to tasks arising from this function.

5.2. Private use of these resources is permitted only as provided for in article 1.2.

5.3. However, the following is prohibited during any use (private or not):

- visiting sites that contain pornographic, racist, discriminatory, abusive or offensive material;
- 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 and any other copyrighted material from any illegal source, or if the employee actually knows 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.
- engaging in activities on the HZ network which are illegal according to the criminal code

Article 6. Use of social media

6.1. The Institution supports open dialogue and the exchange of ideas and the sharing of the employee's knowledge with colleagues and third parties through social media. If this concerns work-related topics, the employee should ensure that the profile and the content is consistent with how he would present himself towards colleagues and students in text, image and sound.

6.2. Directors, managers, executives, and others who dictate policy or strategy on behalf of the Institution have a special responsibility when using social media, even if the content is not directly connected to their work. On the basis of their position, they should consider whether they can publish in a personal capacity. They are aware that employees read what they write.

6.3. This article also applies if employees participate in social media from private computers or internet connections, although only insofar as this concerns participation which could affect the work.

6.4. If an employee sets up a social media account which is directly work-related, and was set up in the name of the employee personally, the employee and Institution will upon termination of employment find a fitting solution for the transfer of this profile and the information and contacts it contains.

Article 7. Monitoring and checks

7.1. Checks on the use of the ICT facilities and internet use only take place within the framework of enforcing the rules in these regulations for the goals named in article 1. Prohibited use of operating assets is prevented through technical means as much as possible.

7.2. For the purpose of checking compliance with the rules, data is collected (logged) automatically. 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.

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

7.4. 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 and personal data. In particular, the Institution secures the data recorded for checks against unauthorized access and persons with access to this are contractually bound to confidentiality.

7.5. Some specific control measures that the Institution can take are:

- checks to prevent negative publicity and unwanted behaviour, especially sexual harassment and system and network security checks take place based on filtering of content on keywords. Suspicious messages are automatically returned to the sender;
- checks in the context of cost and capacity management are limited to examining the sources of costs or capacity demand (such as the addresses of internet radio and video sites) based on traffic data. If these websites lead to high costs or inconvenience, they are blocked or throttled without violating the confidentiality of the content of the communication;
- checks on the use of imagery takes place on the basis of third-party complaints or reports, or based on sample checks of imagery which is publicly accessible.

Article 8. Procedure for targeted investigation

8.1. Targeted investigation is undertaken when traffic data or other personal data relating to a specific employee is recorded in the context of an investigation in response to a serious suspicion of a breach of these Regulations by that employee.

8.2. Targeted investigation only takes place after written instructions from the Executive Board. If the investigation does not give rise to further measures, the records will be destroyed.

8.3. In deviation from the previous paragraph, research into the security or integrity of peripherals is performed by system administrators based on specific instructions. Separate consent of the body referred to in paragraph 2 is not necessary. The results of this investigation are only shared with the employee for the purpose of enhancing the security or integrity of peripherals. In case of repetition, the procedure in paragraph 2 will be followed.

8.4. Targeted investigation is initially limited to traffic data from the use of the facilities. If targeted investigation provides further evidence, the Institution may proceed to an examination of the content of communications or stored files. This requires written permission from the Executive Board, which will state the reasons why it is granted.

8.5. Some specific individual control measures that the Institution can take are:

- checks on the leaking of confidential information take place on the basis of sample checking of keywords. Suspicious messages are set apart for further investigation in consultation with the board;
- checks on the violation of the prohibition listed under Article 4, paragraph 3, are performed by two people opening e-mails and reviewing the content as a result of a complaint [or sample checking]. These individuals are bound to confidentiality regarding the content;

8.6. The employee 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 employee 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.

8.7. Employees of the Information and Automation Department only gain access to accounts or computers of employees if the employee 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 employee will in that case be informed afterwards.

Article 9. Rights of the employee with regards to personal data

9.1. The employee 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.

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

9.3. The employee may also further object to the 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.

9.4. The board will not give the employee any assignments or orders regarding privacy-sensitive information and personal data that are inconsistent with these regulations.

Article 10. Consequences of violation

10.1. When acting in violation of these Regulations or the generally applicable legal rules, the board can take disciplinary measures depending on the nature and severity of the violation. These include a warning, reprimand, transfer, suspension and termination of the employment contract. Additionally, the board can decide to (temporarily) suspend access to certain ICT facilities.

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

10.3. In addition to this, the Institution may upon (automated) discovery of a disturbance implement a temporary block of the facility in question. This block will be implemented until it is demonstrated that the cause has been removed. Upon repeat incidents of the cause, disciplinary measures may be taken.

Article 11. Final provision

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