Radboud Universiteit

Acceptable Use Policy for Employees

Code of Conduct for ICT and internet use for employees of Radboud University

Author(s):	R. Sarelse CISO/FG

Version:	2.2
Date:	May 2018

Version	Date	Brief description of changes
1.0	January 2017	Initial version based on SURF AUP model version 4.0 
2.0	February 2018	Incorporation of feedback from the Joint Assembly
2.1	March 2018	Incorporation of feedback from the Executive Board
2.2	May 2018	Incorporation of feedback from the Joint Assembly

Acceptable Use Policy

This document serves as a code of conduct for ICT and internet use by employees of the Radboud University, and it will hereinafter be referred to as the Code of Conduct.

Basis for the code of conduct

The use of internet and ICT resources is necessary for many of the employees at the institution in order to do their job properly. However, there are some risks associated with the use of these facilities, which led to the creation of a code of conduct. In light of these risks, employees are expected to use internet and ICT in a responsible manner.

With this Code of Conduct, Radboud University, hereinafter referred to as "the Institution", establishes rules in regards to the desired use of these company resources. The aim is to strike a good balance between responsible and secure use of ICT and internet, and the privacy of the employee.

The use of social media is becoming increasingly important but can also affect the Institution. This is why the Institution wants to establish certain rules for it as well.

The Institution, as an employer, is authorised to establish rules regarding work performance and good order in the workplace. This Code of Conduct is based on the law as well as on the CAO NU.

Since the Code of Conduct provides for a processing of personal data or monitoring of employee behaviour or performance, the participational body (Works Council) needs to provide its consent. The Works Council consented to the contents of this Code of Conduct on 1 October 2018.

1. Principles

1.1. The Code of Conduct establishes rules regarding the use of the ICT and internet business resources by employees. The purpose of these regulations is to define acceptable use in relation to

- systems and network security, including protection from damage and abuse;
- prevention of sexual harassment, discrimination and other criminal offences;
- protection of privacy-sensitive information, including personal data of employees and students and parents;
- protection of confidential information of the Institution and its employees, and of students and parents;
- protection of intellectual property rights of the Institution and third parties, which includes respecting the licensing agreements that apply within the Institution;
- prevention of negative publicity;
- cost and capacity management.

The institutional information security policy and other information on information security, and other guidelines are available on Radboud University's Information Security pages:

https://www.ru.nl/privacy/english/

Specific IT services or facilities may have specific guidelines that will be published separately. If in doubt about the rules and regulations, contact line management.

1.2. Limited private use of internet and ICT resources is allowed only insofar as work is not negatively impacted.

1.3. The Code of Conduct applies to everyone who is working for the Institution, this includes agency staff and temporary employees. The Code of Conduct also applies to guests of employees.

1.4. The Code of Conduct also applies if you, as a guest, use the network facilities of other institutions whereby access is gained on the basis of the login details of the home Institution (Eduroam).

1.5. In the context of enforcement of this Code of Conduct, the Institution strives for measures that will limit access to privacy sensitive information or the personal data of individual employees as much as possible.

2. Intellectual property and confidential information

2.1. The employee will treat confidential information and privacy-sensitive information, including personal data that they have access to in the context of work, as strictly confidential and will take sufficient measures to guarantee this confidentiality.

2.2. The employee may not infringe on the intellectual property rights of the Institution and third parties and respects the licence agreements as applicable within the institution.

2.3. Control of the information of the Institution rests with the Institution. The employee has no independent control over the information except where it was explicitly granted by the Institution.[1]

2.4. The employee is not allowed to systematically download large amounts of articles from the digital library or systematically copy substantial parts of the files or databases in the digital library[2].

2.5. The employee pays special attention to taking security measures if the work necessitates processing of sensitive information outside the Institution. Sharing via e-mail and storage in non-institutional cloud applications, on external storage media, or private client devices (USB devices, tablets, etc.) needs to comply with conditions as

[1] See also Knowledge protection and exploitation regulations for Radboud Universiteit Nijmegen and the Radboud university medical center

[2] This refers to large numbers of non-manual downloads, to prevent denial of access for the whole University.

set out by Radboud University.
The employee will closely adhere to any regulations drawn up by the Institution in regard to safeguarding the confidentiality. Please see https://www.ru.nl/privacy/english/ and https://www.radboudnet.nl/privacy/english/

2.6. These regulations particularly apply to systems administrators, for whom violation of these provisions is considered a very serious breach of duty, given their special position.

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 their position. Use is therefore connected with tasks arising from this position. Private use of these resources is only allowed as defined in 1.2.

3.2. The employee should always handle the personal login details and any additional authentication resources with great care. Personal passwords and additional authentication resources may not be shared. Suspected abuse of a password can be a cause for systems management[3] to suspend the account immediately.

3.3. The Institution can prescribe systems or software for educational and business purposes, such as an Electronic Learning Environment, an e-mail system, (mobile) applications (apps), Cloud services, or multimedia services. The employee will only use these systems for sharing teaching materials or conducting research and agrees to abide by the applicable limitations and requirements.

3.4. Installing software on a non-personal computer[4] and network facilities of the organisation is not permitted without specific permission from systems management. Connecting servers and active network components (such as access points and routers) is also not allowed without the permission of systems management.

The systems manager can grant the permission with certain conditions, such as a mandatory installation of virus scanners and password protection, to comply with the Code of Conduct.

Connecting private client devices (such as laptops, tablets, and phones) is only permitted on the (wireless) network connections provided for these purposes. The systems manager can further enforce requirements for the use of these connections, such as a mandatory installation of virus scanners and password protection, to comply with the Code of Conduct.

3.5. Saving private files or information on the Institution's systems is permitted, provided that this does not lead to an overload of the storage capacity of these systems or a disturbance of good order on the work floor. It is desirable to save private data in a subfolder named "private" to keep it separated from work data. However, the Institution is not liable for creating backups of such files or information, or providing

[3] This may be the ISC or another approved Radboud University support group
[4] PCs in meeting rooms, halls, corridors, the library, the refectory (De Refter), study rooms, etc.

backup copies during replacement or repair of said systems. The personal U drive is backed up as a network drive, and is therefore recommended over local storage.

4. Use of e-mail and other ICT communication methods

4.1. The e-mail system and the corresponding mailbox and e-mail address are provided to the employee for use in the context of their position. Use is therefore connected with tasks arising from this position.

4.2. Private use of these resources is only allowed as defined in 1.2.

4.3. Usage, private or academic, should not disturb the good order at the Institution and should not be a nuisance to others, infringe on the rights of the Institution or third parties, or impact the integrity and security of the network.

Usage causing a nuisance or disturbance always includes the following[5]

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

4.4. It is preferred that the employee does not use the institutional e-mail address for sending personal e-mails, within the limits of 1.2. The organisation will not block or specifically monitor access to other e-mail services.

4.5. The Institution is only authorised to provide a replacement or supervisor with access to an employee's mailbox or files in case of illness, unexpected long-term absence, or gross negligence on the part of the employee if there is a serious business interest, and where it can be shown that obtaining the employee's consent is impossible, or where the business interest is so strong that permission is not required. They should not, however, give themselves access to folders marked as private, recognisably private e-mails, or e-mails sent to or from a confidential advisor/occupational health officer/HR consultant. If the employee has not marked anything, the Institution can contact a confidential advisor to check the employee's information to enable the identification of private information and to separate it before providing access to the replacement or the supervisor.

4.6. The content of e-mail messages is not checked. This does not apply to automated checks (logging and monitoring) of the security of the e-mail traffic and the network.

[5] Exceptions may be made in very specific cases, such as certain types of conduct which would normally be seen as a nuisance, but which are necessary in the framework of scientific research.

5. Internet usage

5.1. Access to the internet and associated facilities are provided to the employee for use in the context of their position. Use is therefore connected with tasks arising from this position.

5.2. Private use of these resources is only allowed as defined in 1.2.

5.3. However, the following are not permitted during working hours or while using the Radboud University network/internet access:

- undesirable behaviour[6];
- using file sharing or streaming services where this generates excessive traffic in such a way that the availability of the facilities may be compromised;
- downloading films, music, software, and other copyrighted material from any illegal source or where the employee knows that this violates copyright;
- uploading films, music, software, and other copyrighted material for distribution to third parties without the permission of the copyright holders.

6. Use of social media

6.1. Personal data or the sensitive information of others should not be shared via social media.

6.2. The Institution accepts the open dialogue and exchange of ideas, and the sharing of knowledge by the employee with colleagues and third parties through social media[7].

If posting about work-related topics, the employee needs to ensure that the profile and the content is consistent with how they would present themselves in text, image, and sound in front of colleagues and students.

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

6.4. This also applies where employees participate in social media from private computers or internet connections, but only insofar as the participation may affect work.

6.5. In cases where an employee creates a social media account that is directly work related, and it is set up under the employee's name, the employee and the Institution

[6] https://www.radboudnet.nl/radboudservices/vm/calamiteiten/ongewenst-gedrag/

[7] See also: http://www.ru.nl/huisstijl/huisstijltoepassingen/vm-toepassingen/social-media/

will find a suitable solution for the transfer of the profile and the information and contacts contained within it at the end of the contract of employment.

7. Monitoring and review

7.1. Monitoring of the use of ICT facilities and internet use occurs solely in the framework of security and enforcement of the rules from the Code of Conduct for the purposes mentioned in paragraph 1.

7.2. For safety and compliance with the rules, automated data are collected (logged). This information is only accessible to the systems administrators who are directly responsible, and are only provided in anonymised form to other administrators and other controllers. They may decide on further technical measures.

7.3. In cases of a suspected violation of the rules or impact on security, the individual traffic data while using e-mail and internet can be monitored (by order of a supervisor of a systems administrator or CERT-RU). Monitoring content will only take place in the event that a serious violation is suspected.

7.4. When monitoring at the level of traffic data or personal data, the Institution fully observes the General Data Protection Regulations and other relevant laws and regulations. The Institution focuses on safeguarding the data gathered during monitoring against unauthorised access and the people with access are contractually obligated to maintain confidentiality.

7.5. Some specific measures that the Institution can introduce are:

- monitoring to avoid negative publicity and sexual harassment, and monitoring in the context of system and network security based on filtering content by keywords. Suspicious messages will automatically be returned to the sender;
- monitoring in the context of expense and capacity management is limited to using the traffic data to determine the source of expenses or demand for capacity. If these websites lead to large expenses or nuisance, they will be blocked or congested, without violating the confidentiality of the content of the communication;
- monitoring the use of images takes place on the basis of complaints or reports by third parties, or by sampling images that are publicly available.

8. Procedure for targeted investigation

8.1. Targeted investigations are only initiated after a written order of the dean/director of the relevant faculty or the Executive Board, in which the reasons for the investigation are outlined. If the director/dean send out the order, the Executive Board will receive a copy of the order and a report of the results of the investigation.

8.2. A targeted investigation occurs when traffic data or other personal data relating to a specific employee are recorded in the course of an investigation following serious suspicion of a violation of this Code of Conduct by that employee.

8.4. If a targeted investigation uncovers further evidence, the Institution may proceed to evaluate the contents of communication or stored files. The Institution will make every effort to keep the identity of the people who conduct the evaluation confidential. The results of the investigation are recorded under the name of the director. The record will be destroyed if the investigation does not give rise to further measures.

8.5. The director/dean or the Executive Board will inform the employee about the reason, performance, and outcome of the investigation in writing as soon as possible. The employee is given the opportunity to comment on the findings. Postponement of informing the employee is only allowed in cases where informing early would be detrimental to the investigation.

9. Employee rights in regards to personal data

9.1. The employee can turn to the Board[8] in relation to

- the right to information about the processing;
- the right to access their data;
- the right to have inaccuracies in the data corrected;
- the right to removal of the data ("the right to be forgotten");
- the right to restrict data processing;
- the right to object to data processing;
- the right to transfer their data (data portability);
- the right not to be subjected to automated decision-making.

For each of these requests, the employee is informed about the processing of the request within one month.

9.2. The Board will not order or assign any work to the employee that is in violation of the Code of Conduct in relation to privacy-sensitive information and data.

10. Consequences of violations

10.1. When the Code of Conduct or the generally applicable legal rules have been violated, the Board may take disciplinary measures depending on the nature and severity of the infraction. These include a warning, reprimand, transfer, suspension and termination of the employment contract. In addition, the Board can decide whether or not to apply a temporary limitation of access to certain ICT facilities.

[8] By e-mail: mijnprivacy@ru.nl or myprivacy@ru.nl

10.2. Disciplinary action (except a warning) is not taken only on the basis of automated processing of personal data, such as a report from an automatic filter or block. Furthermore, no disciplinary measures will be taken before the employee is given the opportunity to explain their point of view.

10.3. In addition to the above, it is possible that an (automated) report of a nuisance will cause the Institution to instate a temporary block on the particular facility based on the decision of an authorised person[9]. This block will be maintained until the cause of the nuisance has been remedied. If the nuisance is repeated, disciplinary action may be taken.

11. Final provision

11.1. This Code of Conduct is evaluated once every four years, or in the interim where necessary, by the Board and other parties such as the participational bodies.

11.2. The organisation can change this Code with the consent of the participational body (Works Council) if circumstances give rise to this. Proposed changes are made known to the employees prior to their implementation. The Board will take feedback from employees into consideration before implementing the changes.

11.3. The Executive Board will decide on cases for which this Code of Conduct does not provide.

[9] This may be CERT-RU, a supervisor, etc.