Radboud Universiteit

Acceptable Use Policy for Students

Code of Conduct for ICT and internet use for students at 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 model for AUP students 
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 for Students

Radboud University (hereinafter: the Institution) provides their own students and visiting students access to the internet for academic purposes. Additionally, an institutional mailbox and facilities to save files and personal academic information are made available to students for personal use and academic purposes.

The use of these facilities is bound by regulations to ensure a good state of affairs in the buildings and on the grounds of the Institution. The regulations and possible sanctions are described in this code of conduct, hereinafter referred to as the Code of Conduct.

The Student Council approved the contents of this Code of Conduct on 2 July 2018.

1. Use of facilities

Computer and network facilities (such as public computers, wireless and wired network connections, e-mail and internet access, storage capacity, printers, and electronic learning environments) are made available to the student for academic purposes, such as completing assignments, reports, and theses, administration of study progress, consulting sources, and communicating with teachers and fellow students.

The use of one's own equipment and applications in conjunction with the facilities of the Institution is permitted as long as this use complies with the rules of this Code of Conduct. Changing settings on devices and in applications made available by the Institution is only allowed with specific permission from systems management[1]. Connecting personal networking equipment that allows sharing the connection to the wired or wireless network with a third party is prohibited at all times.

This 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).

Certain facilities are only accessible using a username and password. These are strictly personal and may not be shared with others. Systems management may impose additional requirements on the quality of passwords and other security aspects, as further set out in the Information Security Policy. Suspected abuse of a password or authentication method may be cause for systems management to suspend the account immediately.

2. Intellectual property and confidential information

The student may not infringe on the intellectual property rights of the Institution and third parties and respects the licence agreements applicable within the Institution[2].

[1] This may be the ISC or another approved Radboud University support group.

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

Control of the information of the Institution rests with the Institution. The student has no independent control over the information except where it is explicitly granted by the Institution.

The student 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.[3]

If the student gains access to confidential or sensitive information, including personal data, during the course of his studies or while performing tasks for the Institution, the student should treat this information as strictly confidential.
The student pays special attention to taking security measures such as described in this Code of Conduct if performing tasks necessitates the 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 set out by Radboud University.

The student needs to fully comply with any regulations established by the Institution in relation to safeguarding security and intellectual property rights.

Radboud University's Information Security Policy and more information about information security and other guidelines are available on Radboud University's Information Security pages:

https://www.ru.nl/privacy/english/ and https://www.radboudnet.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 the service desk or the ISC Helpdesk.

3. Institution and student responsible for security

The Institution takes information security seriously. It employs a strict security policy and takes appropriate technical and organisational measures to protect the infrastructure from loss, theft, criminal activities, confidentiality breaches, infringement of privacy rights, and infringement of intellectual property rights.

Of course, no security is perfect. The Institution therefore expects students to have a proactive attitude and to take serious steps to keep their own computer and other devices (such as smart phones or tablets) secure. The student is solely responsible at all times for the use of their own devices and the data stored on such devices.

Additionally, if the student intends to use their device in conjunction with the institutional facilities, in the context of security, they will need to:

- install an adequate virus scanner and firewall on the device;

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

- regularly back up all relevant data and safely store this copy only for as long it is needed;
- use passwords that are difficult to guess and change them regularly;
- keep the software settings on the device up to date;
- use encryption.

4. Private use and nuisance

Limited private use of the facilities is allowed. 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[4]:

- in public spaces, consulting internet services with pornographic, racist, discriminatory, offensive, or objectionable content or sending messages with such content[5];
- sending messages with (sexually) intimidating content or messages that may incite discrimination, hatred, or violence;
- sending messages to large numbers of recipients at once, sending chain letters, or spreading malicious software such as viruses, worms, Trojan horses, and spyware;
- 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 student is or should be aware that this violates copyright;
- uploading films, music, software, and other copyrighted material for distribution to third parties without the permission of the copyright holders.

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

5. Monitoring by the Institution

Monitoring the use of the facilities only occurs in the context of security and enforcement of the rules from this Code of Conduct, to ensure a good state of affairs at the Institution, and

[4] 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 context of scientific research. See also https://www.radboudnet.nl/radboudservices/vm/calamiteiten/ongewenst-gedrag/

[5] https://www.radboudnet.nl/publish/pages/852221/17_6_2_protocol_ordemaatregelen_ru_2017_def_zonder_06nr.pdf

to safeguard the integrity and security of the network and computer facilities of the Institution.

Data is automatically collected (logged) for the above-mentioned purpose of monitoring security and enforcing rules. These data are accessible to the systems administrators who are directly responsible. They may decide to take technical measures such as blocking access to a particular service or limiting the network access capabilities of a device with a view to preventing further problems.

Specifically, if student devices cause a disturbance, steps can be taken to turn off the network access facilities. Where possible, students are warned in advance, so that they have the opportunity to rectify the problem. If urgency prevents a warning in advance, students should be notified of the measure as soon as possible afterwards.

In cases of a suspected violation of the rules or impact on security, the individual traffic data while using the facilities can be monitored. Content will only be monitored in the event that a serious violation is suspected and by order of CERT-RU[6] or the manager of a systems administrator.

When monitoring at the level of traffic data or content, 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 the confidentiality.

6. Procedure for targeted investigation

Targeted investigations are only initiated after a written order from the director/dean of the 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.

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

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.

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

[6] Computer Emergency Response Team of Radboud University

7. Rights of the student in relation to personal data

The student can turn to the Board[7] 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 student is informed about the processing of the request within one month.

8. Consequences of violations

When this Code of Conduct or the generally applicable legal rules have been violated, the Board of the Institution can take disciplinary measures depending on the nature and severity of the infraction. These include a warning, a reprimand, a temporary revocation or restriction of access to facilities (up to one year), and in extreme cases a termination of registration as a student.

Disciplinary action (except a warning) is not automatically taken on the basis of automated processing of personal data, such as a report from an automatic filter or block. The student will have the opportunity to present their standpoint on matters first.

Contrary 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. This block will be maintained for up to a week or shorter if systems management deems that the cause of the nuisance has been rectified. If no improvement has been detected by systems management after a week, systems management can decide to extend the block. If the nuisance is repeated, disciplinary action may be taken.

9. Final provisions

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. Changes are only implemented at the start of the academic year, except in urgent cases or when the Institution is forced to expedite implementation by circumstances outside its control.

---

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

Changes are only implemented after prior approval from the participational bodies. The Board will take feedback from students into consideration before changes are implemented.

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