Radboud Universiteit

Radboud University Code of Conduct for Information Services

Date 13 november 2025

Subject **Gedragsregels informatievoorzieningen**
Version 3.2
Classification Internally, all staff & students
Owner Executive Board
Approved by Executive Board
Aligned with University Joint Assembly (UGV)
Radboud University Director's Meeting (RUDO)

Radboud University

Approval & version control

Name/title	Date adopted	Approved version
Executive Board	15-12-2025	3.2

Agreement

Name/title	Date adopted	Approved version
University Joint Assembly (UGV)	13-10-2025	3.2

Version	Author	Date	Summary of adjustments
1.0	<Redacted>	01-01-2017	First version based on SURF Model Acceptable Use Policy version 4.0
2.8	<Redacted>	15-05-2025	SPA comments processed
2.9	<Redacted>	15-07-2025	RUDO comments processed
2.91	<Redacted>	24-07-2025	Comments from employment and privacy lawyers processed
3.0	<Redacted>	28-07-2025	Version without comments for adoption
3.01	<Redacted>	12-08-2025	Comments AM processed
3.02	<Redacted>	22-09-2025	Questions/comments GV committee VIP processed
3.1	<Redacted>	23-09-2025	Version without comments for adoption
3.2	<Redacted>	31-10-2025	Proposal Article 9 GV adopted

Radboud Universiteit
Houtlaan 4
6525 XZ Nijmegen

P.O. Box 9102
6500 HC Nijmegen
Nederland
www.ru.nl

1. Introduction

1.1. The processing of data and the use of information services, the internet and social media is necessary for work and study but leads to risks for people and Radboud University. The university is responsible for limiting these risks. This is done by, among other things, setting rules of conduct that all users must adhere to (obligation). This document (hereinafter: the Code of Conduct) describes these rules of conduct and serves as an agreement for the use of information facilities between Radboud University and the user.

1.2. For a further explanation of the detailed rules of conduct, please visit the Radboud University website: Policies and regulations | Radboud University.

2. Scope

2.1. The Code of Conduct applies to all employees, students, trainees, volunteers, guests, temporary workers, self-employed persons and employees of third parties (hereinafter referred to as "users") who have access to the information facilities at Radboud University.

2.2. The code of conduct prescribes how data is processed and how Radboud University's information facilities should be used.

2.3. Information facilities include in any case:

A. All information and ICT services (laptop, workplace, telephone, printers, storage, etc.) offered by Radboud University.

B. All forms of internet access provided by Radboud University.

C. Services from other providers insofar as they are used in formal and informal (work) processes of Radboud University. Think of SaaS-services[1] and social media.

2.4. The rules of conduct also apply to all users who, at the time they (as a guest) use the information facilities of other institutions, where access is obtained on the basis of the login details of the institution (such as Eduroam, SURFconext). In such a case, users must always honour the rules of conduct and other rules and guidelines of the other institution.

2.5. Certain information facilities, or types of processing such as the processing of personal data in scientific research, may have additional guidelines that are published separately. In case of doubt about the guidelines and regulations, please contact the administrator of the information provision.

3. Objectives

3.1. The rules of conduct determine the good order for the use of information facilities with regard to:

- system and network security, including protection against damage and misuse;

[1] https://nl.wikipedia.org/wiki/Software_as_a_Service

- combating sexual harassment, discrimination and other criminal offences;
- protection of privacy-sensitive information, including personal data, that the users of the Code of Conduct have to deal with in their (Radboud) activities;
- protection of confidential information[2] of the Institution or its users;
- protection of the intellectual property rights of the Institution and third parties, including compliance with the licensing agreements applicable within the Institution;[3]
- preventing negative publicity;
- cost and capacity control.

3.2. Safety guidelines and other information are available on the Institution's safety pages.[4]

4. General provisions

4.1. Limited private use of the information facilities is permitted insofar as this does not harm the work and the availability, integrity and confidentiality of the information facilities, and does not conflict with applicable laws and guidelines.

4.2. In the context of information security, the Institution strives for the best possible level of knowledge and awareness of its users in the areas to which these rules of conduct refer.

4.3. The user must handle information, including personal data, to which he has access in the context of the work, in a proper manner and take sufficient measures to ensure its availability, integrity and confidentiality. The required organisational and technical measures arising from directives and legislation, including the General Data Protection Regulation and AI Act, are also taken into account.[5]

5. Intellectual Property and Confidential Information

5.1. The user may not infringe the intellectual property rights of the Institution and third parties and must respect the licensing agreements as applicable within the Institution.

[2] If knowledge by unauthorised persons may cause damage to the Institution and may be contrary to the interests of the Institution or users.

[3] See, for example, General rules for the protection of knowledge and knowledge exploitation | Radboud University.

[4] Knowledge security, information security and privacy | Radboud University.

[5] AI in Education | Radboud University.

5.2. Control over the information of the Institution rests with the Institution. The user has no independent control over the information unless explicitly assigned to do so by the Institution.[6]

5.3. The user is not permitted to systematically download and/or large numbers of articles from the files of the digital library and/or to copy substantial parts of the files or databases in the digital library.[7]

5.4. The user pays particular attention to taking measures if the processing of information outside the Institution is necessary in the context of carrying out the work or study. Sharing via e-mail, storage in non-institutional Cloud applications, on external storage media or own client equipment (USB devices, tablets, etc.) must comply with the conditions and legislation set by the institution (including the GDPR).[4]

5.5. If the Institution has drawn up regulations in the field of knowledge security, information security, and/or privacy with regard to guaranteeing confidentiality, the user will strictly comply with them.

5.6. Despite their special position, these provisions also apply to system, application and functional administrators, for whom violation of these provisions is considered a very serious breach of duty.

6. Use of information facilities

6.1. Information facilities and equipment are made available to the user for use in the context of his function or study. Use is therefore linked to tasks arising from this position. Private use of these resources is only permitted as provided for in 4.1.

- The user is not permitted to download or install software that is not prescribed by the Institution on the equipment and information provided without the permission of the Institution.

6.2. Only other services may be used for which the institution has authorised the use.

6.3. The user must at all times handle login details assigned to him personally and any additional means of authentication. Personal passwords and additional means of authentication may not be shared.

- If a password is suspected, the institution can immediately make the account in question inaccessible.

[6] See also General rules for the purpose of Knowledge Protection and Knowledge Exploitation of Radboud University Nijmegen.

[7] This refers to huge numbers that are not downloaded manually in order to prevent the entire institution from being cut off from access to a publisher/database.

- Authorized sessions on facilities are not left unattended by the user. An authorized session on a service is terminated by logging out or locking the session immediately after the related activities.

6.4. The Institution may prescribe systems or applications on the website for educational, research and business purposes, such as storage systems, data processing systems (such as a computing cluster), an electronic learning environment, an e-mail system, (mobile) applications (apps), cloud facilities or multimedia services. The User shall not use any other services for such explicitly prescribed applications and shall also strictly comply with the terms and conditions set therein.

6.5. Installing software on the institution's non-personal computer[8] and network facilities is not permitted without the explicit permission of the administrators[9]. Connecting servers and active network components (such as access points and routers) is also not allowed without permission from the network management i-column[10] and the connection conditions must also be met[11] and the relevant maintenance standards and processes must be followed.

- The Institution may attach mandatory conditions to the consent in order to enforce the rules of conduct.
- Connecting your own client equipment (such as laptops, tablets and telephones) is only allowed on the (wireless) network connections made available for this purpose. The Institution may attach conditions to access to these connections in order to enforce the rules of conduct.
- It is forbidden to use Radboud University facilities (including equipment) commercially (e.g. cryptominers, commercial websites, etc.).

6.6. The user is not permitted to gain or attempt to gain access to computer systems or applications for which no implicit (general) or explicit access option has been created specifically for the user. Conducting security research or pen tests on the Radboud University network or having them carried out without permission from Radboud University is also prohibited.

6.7. Causing damage to the network, systems or services (facilities), due to intent or deliberate recklessness on the part of the user, is not permitted.

6.8. The user is obliged to follow instructions from the administrator responsible for the provision of information.

[8] PCs in meeting rooms, hall, corridor, library, refectory, study rooms, etc.

[9] ILS connectivity, C&CZ, Donders institute, TSG FSW or C&F operators for their equipment

[10] ILS connectivity, C&CZ, Donders institute of TSG FSW

[11] These can be requested from the architects of ILS.

Use of e-mail and other means of communication

6.9. The use of e-mail and other means of communication must not be disruptive to Radboud University and may not cause nuisance to others, infringe the rights of Radboud University or third parties, or affect the integrity and security of the infrastructure, such as the network.

- Disruptive and/or nuisance use is in any case understood to mean[12]:
  - sending messages with pornographic, racist, discriminatory, threatening, insulting or offensive content;
  - sending messages with (sexually) harassing content;
  - sending messages that (may) incite discrimination, hatred and/or violence;
  - sending unsolicited messages to large numbers of recipients, sending chain letters or sending malicious software such as viruses, Trojan horses or spyware.

6.10. The user will only use the e-mail address provided by Radboud University for private e-mail, within the limits of 4.1. Radboud University will not block access to other e-mail services or monitor the content unless there is a disturbance or nuisance, see 6.9.

6.11. Students must use the mailbox and associated e-mail address provided by Radboud University for all applications in the context of their studies.

6.12. It is mandatory to use the Radboud email address and calendar instead of private email services and private calendars for work for Radboud University or study.

6.13. It is not permitted to forward e-mail automatically from the Radboud University mailbox to external mailboxes.[13]

- Actively encouraging the forwarding of e-mails to a private e-mail address, for example by using automatic replies, is not permitted.

6.14. In the event of illness, unexpected long-term absence or gross negligence on the part of the user, Radboud University is entitled to provide a substitute or manager with access to the necessary work-related information (such as files or mailboxes) only if this is strictly necessary for the continuity of education, research or business operations. Access is only granted if prior consent from the user proves impossible or if the compelling business interest justifies this. However, the latter may not gain access to folders marked as private, e-mails that are recognizable as private, or e-mails sent to or from a confidential advisor/company doctor/HR consultant/ombudsperson, integrity officer and trade union official. If the user has not placed such markings, Radboud University will check the user's relevant information by engaging a confidential adviser in order to recognise private

[12] In very specific cases, this can be deviated from, for example certain behaviours that are normally experienced as disturbing, but which are necessary in the context of scientific research. Please contact the Faculty Business Security Officer in advance.

[13] The automatic forwarding of emails to external mailboxes, for example via a filter, is not allowed.

information and place it separately before the replacement or manager receives the necessary information.

6.15. The content of e-mail messages is not monitored. This does not apply to automated checks (SPAM filtering, logging and monitoring) on the security of e-mail traffic and network.

6.16. The user is expected to consult his or her Radboud University mailbox, Radboud website and Radboud news items with some regularity and can therefore not invoke ignorance of communications made.

6.17. The user is expected to respect the current policy on the use and deployment of information facilities at or on behalf of Radboud University.

Use of the Internet

6.18. The following are prohibited when using the network/internet connection of Radboud University:

- undesirable behaviour, see also 'Conflicts and undesirable behaviour' on the website[14];
- use file-sharing or streaming services where this causes a nuisance to generate a lot of data traffic, in such a way that it may jeopardise the availability and normal operation of the facilities;
- download copyrighted material (including but not limited to films, music, software, articles, literature) without having the rights or if one can suspect not having the rights;
- distribute (upload) films, music, software and other copyrighted material, such as articles and books, to third parties without the permission of the rights holders.

6.19. For the performance of work related to Radboud University, do not use networks of which the confidentiality is not known, or of which you may have doubts. Examples are: public networks in trains, airports, terraces, etc. This risk can be reduced by using a VPN connection from the VPN solution prescribed by Radboud University.

Use of data storage facilities

6.20. The storage of private files or information on Radboud University systems is discouraged, if it does happen, it should not lead to an overload of the storage capacity of these systems and under the strict condition that private data in a folder called 'private' is separated from work data. Radboud University is not obliged to make backup copies of such files or information or to make copies available, as is the case with replacement or repair of the systems in question.

6.21. It is forbidden to store pirated software, copyrighted material without a license, or malicious software.

[14] Radboud University undesirable behaviour,

6.22. Personal data and sensitive information must be secured and accessible only by authorized persons (see 'Securely sharing and storing files' on the security page on the website).[15]

6.23. Users are responsible for maintaining their stored data on a regular basis, including deleting any outdated or unused files.

6.24. Deletion of data must be done carefully, ensuring that confidential data is permanently and securely erased.

6.25. You are not allowed to use private storage systems for work-related data storage.

7. Use your own equipment

7.1. The user is[16] allowed to use their own equipment under the terms described in the policy. The user is at all times responsible for the use of his own equipment and the data stored on this equipment.

7.2. If the user uses their own equipment at Radboud University's facilities, they must follow the policy in the context of security.[17]

8. Working from home / working remotely

8.1. The user avoids logging in to and via computers that do not belong to or to Radboud University.

8.2. The user always uses the VPN prescribed by Radboud University if it is necessary to make a secure connection to the company network.

8.3. As a user, only use secure and encrypted Wi-Fi connections. If this is not possible, always use a VPN on public Wi-Fi networks.

8.4. The user provides a safe and shielded workplace to prevent unauthorized access to equipment and information.

- The user locks his or her screen when leaving the workplace (for a while) and does not leave any confidential and/or privacy-sensitive information visible.

[15] Share and store files securely,

[16] These rules of conduct, as well as the information security policy,

[17] Policy for securing own mobile apparaten.pdf in the policy portal.

9. Use of social media

9.1. Radboud University accepts the open dialogue and the exchange of ideas and the sharing of knowledge of the user with peers and third parties via social media. If these are work-related topics that fit the employee's profile, the employee must ensure that the profile and content are in line with how they would present themselves in text, image and sound to colleagues and students. This does not mean statements that are clearly made in a personal capacity and cannot be associated with Radboud University.

9.2. Personal data (as referred to in the GDPR), confidential business information and/or other sensitive data of third parties may not be shared with unauthorized persons via social media or other channels.

9.3. All employees, including administrators, managers, executives, teachers, and others who propagate policy or strategy on behalf of Radboud University, have a special responsibility when using social media[18], even if the content is not directly related to their work. This also applies to use via private devices or private accounts, insofar as the expressions affect the work or can be associated with it. Given their position, they must carefully consider whether and in what form they can publish statements in a personal capacity or respond. They must be aware that people inside and outside Radboud University read what they write.

9.4. When an employee sets up a social media account that is directly work-related (Radboud University), while it is in the name of the user personally, the employee and Radboud University will look for a suitable solution for transferring this profile or the information and contacts on it upon termination of employment.

10. Use images

10.1. The campus is largely a publicly accessible space. It is permitted to publish images taken on campus with news items, provided that this does not disproportionately infringe on privacy. This falls under 'freedom of news gathering' and applies to news on websites, social media and in print.

10.2. If people are recognisably portrayed at meetings and activities in the buildings or space managed by Radboud University, you should always ask for at least verbal permission in advance. This applies in particular to images of lectures[19], practicals, study workplaces and research activities. For commercial or promotional purposes or for staged images, written permission is required. Examples of declarations of consent can be found on the Radboud University website.[20]

[18] https://www.ru.nl/medewerkers/services/begeleiding-advies-en-klachten/wetenschapveilig/regeling-social-media-radboud-universiteit

[19] Online education and web lectures | Radboud University , House rules Radboud University

[20] Permission photography and visual material.

10.3. People may object to the use of visual material in which they are recognizable. In the event of a valid objection, the images in question in the image bank and, where possible, in publications, will be removed or made unusable, subject to legal obligations.

10.4. Retention periods apply to visual material. After the expiration of the applicable retention period, the photo, video or other image recordings must be deleted or anonymized in line with the internal retention and destruction policy[21].

11. Hailing

11.1. The user is obliged to report to the ICT Helpdesk by telephone or in writing for the following situations:

- In the event of (suspected) a data breach, of personal data and/or business-critical data;
- In the event of (suspected) potential security problems;
- In the event of loss or suspicion of theft of (parts of) equipment and/or assets of Radboud University, e.g. laptops, telephones, hard drives, campus card, etc.

  This also applies to private equipment that contains personal data and/or company data of Radboud University.

12. Monitoring in control

12.1. Monitoring of the use of the ICT facilities and internet use takes place in the context of security and enforcement of the rules from the code of conduct for the objectives referred to in paragraph 3. See also the policy for logging in the policy portal.

12.2. For the purpose of checking security and compliance with the rules, data is collected (logged) automatically. This data is only accessible to the directly responsible system administrators and the personnel of the Security Operating Center (SOC) and is made available in pseudonymised form to other administrators and other controllers.

12.3. In case of suspicion of violation of the rules or security, an ILS director or the Chief Information Security Officer (CISO) can[22] be ordered to carry out an inspection at the level of individual traffic data of e-mail and internet use.

12.4. Only if there are compelling reasons for checking the content will be carried out in accordance with the applicable procedure, see paragraph 13.

12.5. When checking the level of traffic data or personal data, Radboud University fully complies with the General Data Protection Regulation and other relevant laws and regulations. In particular, Radboud University protects the data recorded during the audit against

[21] See the retention and destruction policy and guidelines on knowledge security, information security and privacy | Radboud University.

unauthorised access and persons with access to it are contractually obliged to maintain confidentiality.

12.6. Some specific control measures that Radboud University can implement are:

- control to prevent negative publicity and sexual harassment. The control in the context of system and network security is carried out on the basis of keyword filtering of the content. Suspicious messages are automatically returned to the sender;
- Control in the context of cost and capacity control is limited to the identification of the sources of costs or capacity demand on the basis of traffic data. If these websites lead to major costs or inconvenience, they will be blocked or throttled, without violating the confidentiality of the content of the communication;
- Checks on the use of visual material take place on the basis of complaints or reports from third parties, or on a random basis for visual material that is publicly available.

13. Procedure for targeted investigations

13.1. Targeted investigation occurs when traffic data[23] or other personal data relating to a specific user are recorded in the context of an investigation following a serious suspicion of a violation of the rules of conduct by that user.

13.2. Targeted research will only take place after a written order from the dean/director of the relevant faculty, unit or the Executive Board, stating the reasons why it is provided. If it is done on behalf of the dean or director, the Executive Board will receive a copy of this assignment and a record of the results of the research.

13.3. If targeted research yields further evidence, Radboud University may proceed to take note of the content of the communication or stored files. Radboud University will make every effort to keep the identity of the persons carrying out this knowledge confidential. The results of the investigation are recorded under the name of the dean or director. If the investigation does not give rise to further measures, the records will be destroyed.

13.4. The user[24] will always be informed in writing as soon as possible by the dean, the director or the Executive Board about the reason, the conduct and the result of the investigation. The user is given the opportunity to explain the data found. A short postponement of informing is only allowed if informing would actually harm the investigation.

14. Consequences in case of violation

14.1. In the event of acting in violation of the Code of Conduct or the generally applicable statutory rules, the Executive Board/Dean or Director may, depending on the nature and

[23] All data related to or resulting from the use of ICT facilities, which do not concern the content of files or messages.
[24] If the user wishes to object to targeted research, there are objection or appeal options for employees and/or students, depending on the situation within the university.

seriousness of the violation, (temporarily) restrict or revoke access to buildings, systems or facilities, and/or take disciplinary, orderly and/or employment law measures.

This includes, among other things, a verbal and/or written warning, reprimand, a temporary closure or restriction of the facilities (maximum 1 year), withholding a promotion and/or salary increase, transfer, suspension, suspension and termination of the employment contract, with or without immediate effect (instant dismissal) or termination of enrolment as a student.

14.2. Disciplinary action (other than a warning) is not based solely on an automated detection or processing of data, such as an automatic filter notification or a block. Before a measure is imposed, the user concerned is always given the opportunity to express his or her views.

For employees, in the event of (a suspicion of) a violation, the manager and HR are in any case involved. For students, the procedure laid down in the Student Charter is followed.

14.3. If (automated) detection of nuisance occurs, an authorised person may decide on behalf of Radboud University to temporarily block access to the facility in question. This measure will only be applied to the extent necessary to end the nuisance and will remain in force until it has been demonstrated that the cause has been removed.

In the event of repetition or persistence of the violation, appropriate disciplinary and/or orderly measures may be taken in accordance with the applicable procedures.

15. Final provisions

15.1. These Rules of Conduct are evaluated once every 5 years or if there is reason to do so in the interim, by the Executive Board and other parties, such as the (competent) participation body.

15.2. Radboud University may amend these rules of conduct with the consent of the competent participation body if circumstances give cause to do so.

15.3. References to relevant web pages will become up-to-date as soon as possible without an approval procedure.

15.4. In cases not provided for in the Code of Conduct, the Executive Board decides.