UNIVERSITEIT VAN AMSTERDAM

RULES FOR THE RESPONSIBLE USE OF ICT FACILITIES BY STAFF OF THE UNIVERSITY OF AMSTERDAM

Laid down by Order of the Executive Board No 2018-068316 on 25 September 2018

Basis for the Rules for the responsible use of ICT facilities

For many staff at the University of Amsterdam ('***the UvA***'), the use of ICT facilities[1] is necessary to complete their work properly. However, there are risks associated with the use of these facilities. Against the background of these risks, UvA staff are expected to use ICT facilities responsibly.

With these Rules for the responsible use of ICT facilities ('the Rules'), the UvA intends to lay down rules for the desirable use of its ICT facilities. It aims to strike a good balance between the use of ICT facilities for teaching, research and operational purposes, the safe and responsible use of ICT facilities, and the staff member's privacy. The mission of the UvA is to provide a university education for the vanguard of tomorrow, to conduct ground-breaking fundamental and applied scientific research, and to translate the results into relevant practical applications for society. Responsible use of ICT facilities supports staff and students to achieve this mission, within an institution where the freedom of staff and students to act is of great importance.

While the use of social media is increasingly important, it can also have repercussions for the UvA. Accordingly, these Rules include certain rules of conduct for social media use.

The UvA is the owner of the ICT facilities made available to its staff and is entitled in that capacity to set conditions on staff use of those facilities.
In addition, staff members are bound by these Rules pursuant to Section. 125 ter of the Civil Service Act (*Ambtenarenwet*) and Article 1.8(2) of the Collective Labour Agreement for Dutch Universities (CAO NU) (after the introduction of the Civil Servants (Normalisation of Legal Status) Act (WNRA), also pursuant to Section 7:611 of the Civil Code).

These Rules will take effect on 25 September 2018 following the approval of the Central Works Council (pursuant to Section 27(1)(d) of the WOR) on 30 August 2018.

Article 1. Guiding principles

1.1 These Rules govern the use of ICT facilities by UvA staff. The purpose of these rules is to set out the proper procedures with regard to:
- safeguarding system and network security, including protection from damage and misuse;
- combating sexual harassment, discrimination and other criminal offences;
- protecting personal data;
- protecting confidential information;
- protecting intellectual property rights and respecting licence agreements;
- avoiding a false image of the UvA through the dissemination of inaccurate information;
- managing costs and capacity.

1.2 Limited private use of ICT facilities is permitted, provided that work tasks do not suffer, it is not disruptive to others and it does not have a disruptive effect on the smooth operation – including the availability – of the network or other ICT facilities.

1 'Other ICT facilities' include hardware, software and information systems.

1.3 These Rules apply to everyone who works at the UvA, temporary employees and guests.[2] The Rules do not apply to students, including visiting students, to whom the separate Student Rules apply.
1.4 These Rules also apply to staff members who make use of the network facilities of other institutions to which access is obtained as guest users using login details from their own institution (e.g. eduroam).
1.5 In enforcing these Rules, the UvA will strive to employ measures that minimise access to personal data. Where possible, the UvA will use only automated monitoring and filters, without personally accessing or giving third parties the ability to access data on the behaviour of individuals.

Article 2. Intellectual property and confidential information

2.1 Staff members must ensure strict confidence in handling confidential information, including personal data, and take adequate measures to preserve confidentiality.
2.2 Staff members must not breach intellectual property rights and must respect licence agreements.
2.3 Staff members have no control or power of disposal over the UvA's property, except to the extent that it has been explicitly granted to them.
2.4 Staff members are not permitted to download large numbers of articles from the files of the digital library or systematically copy substantial portions of files or databases in the digital library.[3]
2.5 If it is necessary in the course of performing work tasks to process confidential information – including research data and/or personal data – outside of the Institution (e.g. via email, in non-UvA cloud applications, or on external storage media or staff members' own devices or storage media, such as USB devices or tablets), staff members must pay special attention to the application of security measures. The UvA may set additional conditions on the permissibility and/or manner of storing, sending and sharing messages and files. Staff members must comply with any such additional conditions.
2.6 These provisions apply in particular to staff members working in operational, applicational or functional management of an information system , for whom a breach of these provisions will be regarded as an extremely serious dereliction of duty, in view of their special position.

Article 3. Use of ICT facilities

3.1 ICT facilities are made available to UvA staff for use in the context of their positions. Use of these facilities is therefore connected to the tasks associated with their position. Private use of the ICT facilities made available by the UvA is permitted only as described in Article 1.2.
3.2 Staff members must take care of their allocated personal login details and any additional means of authentication (such as smart cards and tokens) at all times. Personal passwords and additional means of authentication must not be shared. In case of suspected misuse, the UvA may immediately block access to the associated account.

---

2 People who perform work at the UvA in any capacity and/or contribute to teaching and research (such as trainees, people connected to units in the context of research or exchange programmes, seconded staff and/or persons working on an expense claims basis).
3 This article assumes that the files in the digital library are subject to copyright restrictions. In light of open access developments, this provision may be less relevant.

3.3 For teaching and other operational purposes, the UvA may stipulate the use of certain systems or applications, such as an electronic learning environment, an email system, mobile and other applications (apps), and cloud and multimedia services. In this case, staff members may use only these systems to share teaching materials or conduct research, and must strictly comply with the associated restrictions and requirements.

3.4 With regard to the use of ICT facilities, staff members are specifically prohibited from:

a. accessing or attempting to access the data of other staff members or the software files of computer systems, or altering or destroying them, unless they are expressly given verifiable consent to do so;
b. accessing or attempting to access computer systems, where no explicit means of access to these systems has been created for the staff member;
c. taking any actions that undermine the integrity and continuity of ICT facilities;
d. making unauthorised attempts to obtain higher privileges for ICT facilities than those that have been granted;
e. making unauthorised attempts to obtain system or user authorisation codes (such as passwords) in any way and in any form;
f. reading, copying, altering or erasing emails and other messages intended for other people;
g. copying the software, data files and documentation made available by the UvA, or giving third parties access to them, unless given written consent to do so;[5]
h. intentionally, or through culpable acts or omissions, introducing computer malware[6] (or other malicious software) to or via ICT facilities.

3.5 Installing software in the UvA's ICT facilities is not permitted without the consent of ICTS, unless general consent to install components yourself is part of the service provided by ICTS.

3.6 Connecting servers and active network components to the UvA network (such as access points and routers) is not permitted without the consent of ICTS.

3.7 Connecting personal devices (such as laptops, tablets and phones) is permitted only at the wireless or other network connection points made available for that purpose. ICTS may design rules for access to these connection points for the purpose of enforcing these Rules, such as a requirement to install virus scanners and password protection.

3.8 The storage of private files or information on the UvA's systems is permitted, provided that it does not overload the storage capacity of these systems or disrupt smooth operations in the workplace. However, the UvA is not obliged to make backup copies of such files or information, or to make copies available if the systems in question are replaced or repaired.

3.9 The use of ICT facilities by staff members in connection with activities outside of their employment is permitted only if and to the extent that the UvA has given its written consent.

Article 4. Use of email and other ICT communication tools

4.1 The email system, as well as the associated email account and email address, are provided to staff members for use in the context of their position. As a result, their use is connected to the tasks associated with such positions.

4.2 Private use of the email account is permitted only as described in Article 1.2.

5 In the case of open source files, written consent is not required. The open source licence conditions are considered to constitute the giving of written consent.

6 Malware is malicious software being used to disrupt a computer system intentionally. The purpose of malware varies from making the system unusable to gathering information.

4.3 However, sending information or messages that could harm the image or the moral or economic interests of the UvA is prohibited during both private and work-related use of ICT communication tools.[7] Examples include:
- sending messages with pornographic, racist, discriminatory, threatening, offensive or indecent content;
- sending messages with intimidating content, including content that amounts to sexual intimidation;
- sending messages that incite or could incite discrimination, hate and/or violence;
- sending unsolicited messages to large numbers of recipients and sending chain letters or malicious software (malware).

4.4 Staff members should preferably refrain from using the email address allocated by the UvA for private emails, within the scope of Article 1.2.

4.5 In case of illness, an unexpected long-term absence or gross negligence on the part of a staff member, but only if it provides a compelling reason to obtain access in the UvA's interests, the Institution is entitled to give a substitute or manager access to the files or email account of the staff member, but only if it can be shown that it is impossible to obtain the consent of the staff member or the UvA's interests are so urgent that consent cannot be requested. However, the Institution may not give access to any folders marked as private or emails which are recognisable as private, or send or receive emails to or from a confidential adviser/occupational physician/HR consultant. If the staff member in question has not marked any folders as private, the Institution can ask a confidential adviser to check the staff member's information, identify any private information and place it in a separate folder before the substitute or manager is given access.

4.6 Email messages from fellow members of a representative advisory body, from occupational physicians, from HR consultants and from any other person entitled to invoke confidentiality under the law will not be checked. This provision does not apply to automated checks on the security of email traffic and the network.

Article 5 Internet use

5.1 Access to the internet and associated ICT facilities is provided to staff members in the context of their position. As a result, the use of the internet and associated ICT facilities is connected to the tasks associated with such positions.

5.2 Private use of the email account is permitted only as described in Article 1.2.

5.3 However, the following is prohibited during both private and work-related use of the internet:
- visiting web pages that could harm the image or the moral or economic interests of the UvA, such as web pages that contain pornographic, racist, discriminatory, offensive or indecent material;[8,9]
- obtaining unauthorised access to non-public sources on the internet.

5.4 The ICT facilities made available to staff include file-sharing and streaming services. In the event that the use of these services generates excessive data traffic to the extent that it threatens the availability of the ICT facilities, the UvA may take action to remedy the situation.

---

7 Action will be taken on the basis of complaints from staff and students or other sources (e.g. third parties). Complaints will be assessed on the basis of laws and regulations.
8 The sites described in this article may also be the subject of academic teaching and research. It is of course possible to perform such teaching and research, and access to the sites will be assessed within the ethical considerations associated with that teaching or research.
9 Action will be taken on the basis of complaints from staff and students or other sources (e.g. third parties). Complaints will be assessed on the basis of laws and regulations.

Article 6. Social media use

6.1 The UvA supports open dialogue, the exchange of ideas and the sharing of knowledge by staff members with their peers as well as third parties via social media. Staff members are UvA employees 24/7 and communications on social media can sometimes have unforeseen consequences. All staff members represent the UvA, particularly if the UvA is mentioned as their employer. When using and communicating via social media, staff members will ensure that they make valuable and meaningful contributions, making it clear that they are giving their personal opinions which are not necessarily the same as those of the UvA. Annex 1 of the Social Media Guidelines provides a guide to all staff on the proper use of social media. These Guidelines are available on the UvA website.[10]

6.2 Managers, supervisors and other people who communicate policies or strategies on behalf of the UvA have a particular responsibility with regard to the use of social media, even if the content of their posts does not relate directly to their work. Based on their position, they need to check whether they can publish in their personal capacity. They must be conscious that staff members read what they write.

6.3 This article also applies if staff members participate in social media from private computers or internet connections, but only to the extent that such participation could affect their work.

6.4 If a staff member has set up a social media account that is directly related to their work for the UvA, the staff member and the UvA must find an appropriate solution for transferring this profile or the associated information and contacts when the employment relationship ends.

Article 7. Monitoring

7.1 Monitoring the use of ICT facilities will be done solely in the context of enforcing these Rules for the purposes set out in Article 1. Prohibited use of ICT facilities will be rendered impossible, to the extent that it is feasible to do so using technical means.

7.2 For the purpose of monitoring the functioning of the system and compliance with the rules, data will be collected in an automated manner (logged). These data will be accessible only to the ICT administrators directly responsible, and will be made available to other managers and other persons responsible only in anonymised form.

7.3 In case of a suspected breach of the rules, monitoring may be performed at the level of individual traffic data for email and internet use. Monitoring of content will be done only for compelling reasons.

7.4 With regard to monitoring at the level of traffic data or personal data, the UvA will fully comply with the General Data Protection Regulation (GDPR) as well as other relevant laws and regulations. In particular, the UvA will secure the data collected during monitoring against unauthorised access and persons with access to these data will be contractually bound to secrecy.

7.5 Some of the specific measures that the UvA may perform for monitoring purposes include the following:

- monitoring to prevent leaks of confidential information, as well as monitoring in the context of system and network security, will be based on the filtering of content using keywords. Suspicious messages will be automatically returned to sender;
- monitoring in the context of managing costs and capacity will be restricted to checking the sources of costs or capacity demands (such as addresses of video sites) on the basis of traffic data. If these websites are leading to high costs or nuisance, they will be blocked or cut off, without breaching the confidentiality of the content of the communication;

10 The Guidelines can be found at https://medewerker.uva.nl/content-secured/az/social-media/social-media.html.

- monitoring the use of copyright-protected image material will be based on complaints or reports from third parties, or on random checks for image material that is publicly available.

Article 8. Procedure for specific investigations

8.1 A specific investigation is conducted when traffic data or other personal data on a specific staff member are collected in the context of an investigation in response to a compelling suspicion of a breach of these Rules by that staff member.

8.2 Specific investigations into traffic data or other personal data will be conducted only after written instructions are issued by the Dean (for faculties) or the Director of the relevant department (for other units), following consultation with the Data Protection Officer (DPO) and approval from the ICTS Director. The Executive Board and the Data Protection Officer (DPO) will receive a copy of the instructions as well as a record of the results of the investigation. If the investigation does not give rise to further measures, the records will be destroyed.

8.3 Contrary to the previous paragraph, targeted investigations into the security or integrity of the ICT facilities may be conducted by ICTS based on specific indications. Separate consent from the authority specified in Paragraph 2 is not required. The results of these investigations will be shared with the staff members concerned only for the purpose of improving the security or integrity of the ICT facilities. If the issue recurs, the procedure in Paragraph 2 will be followed.

8.4 In the first instance, targeted investigations will be limited to traffic data on the use of ICT facilities. Should a specific investigation uncover further evidence, the UvA can proceed to examine the content of communications or stored files. This process requires the written consent of the Executive Board; such consent must state the reasons for which it was granted.

8.5 Some of the specific, personal measures that the UvA may perform for monitoring purposes include:

- monitoring for leaks of confidential information, based on random checks using keywords. Suspicious messages will be set aside for further investigation in consultation with the Executive Board;
- monitoring for infringement of the prohibition in Article 4(3), based on a specific complaint. Such monitoring will consist of two people opening email messages and reading the contents. These people are bound to secrecy with regard to the contents.

8.6 Staff members will be informed in writing by the Director of the relevant department as soon as possible of the reason for the investigation, its procedure and its outcome. Staff members will be given an opportunity to provide an explanation of the data found. A delay in informing staff members is permissible only if informing them would cause actual harm to the investigation.

8.7 Authorised ICTS staff may gain access to a staff member's accounts or computers only if the staff member has given their consent. Access without such consent is permitted only in urgent situations or where there is a clear suspicion of a breach of these Rules, as referred to earlier in this article. In that case, the staff member must be informed afterwards.

Article 9. Rights of staff members with regard to personal data

9.1 Staff members may contact the Board to request a full list of their personal data processed by the Institution in the context of these Rules. This request will be fulfilled within four weeks.

9.2 Staff members can request the Board to rectify, supplement, delete or block their personal data if they are factually incorrect, incomplete for their intended purpose or irrelevant, or if they conflict with a statutory requirement.

This request will be responded to within four weeks. If the request is denied, reasons will be given. If the request is granted, it will be acted upon as quickly as possible.

9.3 Staff members can also raise an objection to the processing of their personal data in connection with compelling personal circumstances. The Board will assess whether the objection is valid within four weeks of receipt. If the Board deems the objection to be valid, it will cease the processing in question immediately.

9.4 The Board will not give staff members any tasks or instructions with regard to privacy-sensitive information and personal data that conflict with these Rules.

Article 10. Consequences of a breach

10.1 In case of actions in contravention of these Rules or the generally applicable legal rules, the Executive Board may take disciplinary measures depending on the nature and gravity of the breach. Such measures may include a warning, reprimand, reassignment, suspension or termination of employment. The Executive Board may also decide on temporarily or permanently restricting access to certain ICT facilities.

10.2 No disciplinary measures will be taken without the staff member concerned having an opportunity to present their side of the story.

10.3 Apart from a warning, no disciplinary measures will be imposed if the monitoring was solely based on the automated processing of personal data (such as an observation based on an automatic filter or a block).

10.4 In addition to the above, it is possible that the UvA may implement a temporary block on the ICT facility in question following an automated observation of nuisance. This block will be maintained until it is demonstrated that the cause has been removed. If the cause recurs, disciplinary measures may be taken.

Article 11. Concluding provision

11.1 In cases not provided for by these Rules, the Executive Board will take a decision. Depending on the subject, the Executive Board will take advice from the Chief Security Officer (CSO) and/or the Chief Information Security Officer (CISO) and/or the Data Protection Officer (DPO).