UNIVERSITEIT VAN AMSTERDAM

RULES FOR THE RESPONSIBLE USE OF ICT FACILITIES BY STUDENTS AT 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

The University of Amsterdam ('***the UvA***') offers its own students and visiting students the possibility of using its internet and ICT resources for study purposes. To that end, students are given a UvA email account as well as a location to store files and personal study data.

The use of these facilities is subject to rules in order to ensure the smooth conduct of affairs in UvA buildings and grounds.
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 study purposes, the safe and responsible use of the ICT facilities, and the student'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.

These Rules will take effect on 25 September 2018 following the approval of the Central Student Council (pursuant to Section 27(1)(d) of the WOR) on 5 July 2018.

Article 1. Guiding principles

1.1. These Rules govern the use of the internet and ICT facilities by UvA students. 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;
- managing costs and capacity.

1.2 Limited private use of the internet and ICT facilities is permitted, provided that it does not disrupt the smooth running of the UvA and does not cause a nuisance to others, breach the rights of the UvA or third parties, or have a disruptive effect on the smooth operation – including the availability – of the network or other ICT facilities.

1.3 These Rules apply to everyone who falls into the category of 'Students'.[1] These Rules do not apply to natural persons to whom the 'Rules for the responsible use of ICT facilities by staff of the University of Amsterdam' apply.

1.4 These Rules also apply if use is made of the network facilities of other institutions to which access is obtained using UvA login details (e.g. eduroam).

1 This category concerns both students enrolled at the UvA and visiting students.

1.5 In enforcing these Rules, the UvA will strive to employ measures that keep access to the personal data of individual students to a minimum. Where possible, the UvA will use only automated monitoring and filters, without personally accessing or giving other people the ability to access the behaviours of individuals.

Article 2. Intellectual property and confidential information

2.1 Students will not breach the intellectual property rights of the UvA or third parties and will respect licence agreements.
2.2 Control over the UvA's information is retained by the UvA. Students have no independent control or power of disposal over the UvA's property, except where it has been explicitly granted to them.
2.3 Students are not permitted to download large numbers of articles from the files of the digital library or systematically copy substantial portions of the files or databases in the digital library.[2]
2.4. If students obtain access to confidential information or privacy-sensitive information including personal data in the course of their studies or in the course of performing tasks for the UvA, they must handle that information in strict confidence pursuant to the privacy rules.
2.5 If it is necessary in the course of performing these tasks to process confidential information outside of the Institution, e.g. via email, in non-UvA cloud applications, or on external storage media or students' own devices (USB devices, tablets, and so on), students must pay special attention to the application of the security measures described in these Rules.
2.6 If the Institution has drawn up detailed rules for the safeguarding of confidentiality and intellectual property rights, the student must follow such rules to the letter.

Article 3. Use of ICT facilities

3.1. The ICT facilities such as study centre facilities, wireless and network connections, email and internet access, storage capacity, printers and electronic learning environments are made available to students for study purposes, including for writing assignments, reports and theses; keeping track of their progress; consulting sources; and communicating with lecturers and fellow students.
3.2. Students 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.
3.3 With regard to the use of ICT facilities, students are specifically prohibited from:
a. accessing or attempting to access the data of other users 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 student;
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;

2 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.

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 granted written consent to do so;
h. intentionally, or through culpable acts or omissions, introducing computer malware[3] (or other malicious software) to or via ICT facilities.

3.4 Installing software in the UvA's ICT facilities is not permitted without the consent of ICTS.

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

3.6 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 make 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.

3.7 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.

Article 4. Security measures by the UvA as well as students

4.1 The UvA will apply an information security policy, and take adequate technical and organisational measures, to secure the infrastructure against loss, theft, criminal activities, loss of confidentiality, breach of property rights and breach of intellectual property rights.

4.2 In turn, the UvA expects students to have a responsible and proactive attitude towards the adequate protection of their own computers and other devices (such as smartphones and tablets). Students are responsible at all times for the use of their own devices and for the data stored on these devices.
If students make use of the Institution's facilities using their own devices, it is advisable with regard to the proper management of their own devices to:
- provide their devices with an adequate virus scanner and firewall;
- keep the software settings on their devices up to date;
- make regular backup copies of all relevant data and safely store copies of settings data.

Article 5. Private use and nuisance

5.1 Private use of the internet and ICT facilities is permitted as described in Article 1.3.

5.2 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 study-related use. Examples include:[4]
- accessing internet services with pornographic, racist, discriminatory, offensive or indecent content in public areas, or sending messages with such content;
- sending messages with content that constitutes harassment (including sexual harassment), or sending messages that incite or could incite discrimination, hate and/or violence;

3 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 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.

- sending messages to large numbers of recipients at once, sending chain letters or spreading malicious software such as viruses, worms, Trojan horses and spyware.

5.3 Using computer and network facilities for commercial activities is permitted only when the UvA has given its written consent.

5.4 The ICT facilities made available to students 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.

Article 6. Monitoring by the Institution

6.1 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 the facilities will be rendered impossible, to the extent that it is feasible to do so using technical means.

6.2 For the purpose of this monitoring, automated data will be collected (logged). This data will be accessible only to the ICT ~~managers~~administrators directly responsible, and will be made available to other managers and other persons responsible only in anonymised form.

6.3 Particularly in case of nuisance caused by students' devices, the means of access to the network can be switched off. The students will be warned in advance if possible, so they have an opportunity to stop the nuisance. If it is not possible for reasons of urgency to warn the students before implementing this measure, notification of the measure will be given as quickly as possible.

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

6.5 With regard to monitoring at the level of traffic data or content, 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.

Article 7. Procedure for specific investigations

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

7.2 A specific investigation will take place only after written instructions are issued by the Dean of the Faculty, after consultation with the Data Protection Officer (DPO) and approval by the ICTS Director; such permission must state the reasons for which it was granted. 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.

7.3 In the first instance, specific 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, after obtaining separate consent. If the investigation does not give rise to further measures, the records will be destroyed.

7.4 Contrary to the foregoing, specific investigations into the security or integrity of ICT facilities may be performed by ICT ~~managers~~ management based on specific indications, without separate consent. The results of these investigations will be shared with the students concerned only for the purpose of improving the security or integrity of peripheral devices. If the issue recurs, the procedure in the previous paragraph will be followed.

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

7.6 Authorised ICTS staff may gain access to a student's accounts or computers only if the student 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 student must be informed afterwards.

Article 8. Consequences of a breach

8.1 In case of a failure to follow instructions or directions based on these Rules, or 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, temporary exclusion from or restriction of the facilities (for a maximum of one year) and, in extreme cases, termination of enrolment as a student.

8.2 No disciplinary measures will be taken without the students concerned having an opportunity to present their side of the story.

8.3 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).

8.4 In addition to the above, it is possible that the UvA may implement a temporary block on the facility in question following an automated observation of nuisance. This block will be maintained for a maximum of one week, or less if the cause is removed to the satisfaction of the ICT ~~managers~~management. Should no improvement be noted by the ICT ~~managers~~ management after a week, they may decide to implement a longer block. If the cause recurs, disciplinary measures may be taken.

Article 9. Concluding provisions

9.1 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).