Acceptable Use Policy

UM Student ICT and Internet Regulations.

Version 2.0

17 November 2020

Version	Status	Date	By
1.1	Concept	4 August 2020	CISO
1.2	Concept	5 August 2020	Privacy Team / UM-SOC
1.3	Approval	22 September 2021	University Council
2.0	Adoption	17 November 2020	Executive Board

Table of Contents

Preamble

In the Acceptable Use Policy (AUP), you can read which regulations for ICT and internet use the UM Executive Board has adopted for its students. An AUP is necessary to make it clear to students how they can use UM's ICT facilities for study purposes, without violating (legal) rules and guidelines and without compromising the security of UM's digital systems. Above all without endangering the safety of other users. Finally, the agreements in the AUP also ensure that your rights as a student will be respected.
Therefore, this AUP is available to every student. All users of UM's ICT facilities are expected to familiarize themselves with the UM regulations and the law and, above all, to use their "common sense".

Users of UM ICT facilities reflect society. This means that users can make mistakes or errors and it is even conceivable that unwanted actions are intentionally committed. No regulations can withstand this.
It is of course also conceivable that, despite your precautions, you as a user become the victim of a phishing attack or a virus or malware infection.
This AUP explicitly intends to clarify expectations amongst users and between users and system administrators and to provide a framework for communication about these expectations. Users are asked to continue doing this in an open atmosphere. The chance of errors, mistakes and misunderstandings is thus reduced.

The AUP provides measures for cases of undesirable behaviour. As a rule, this will be a warning explaining why the present behaviour is undesirable and what the consequences of (recurrence) of that behaviour are. It cannot be ruled out that cases will arise in which, in the opinion of the Executive Board, the seriousness of the situation requires more severe intervention and a warning is not sufficient and a more severe sanction is appropriate.
In all cases, the user is given the opportunity to put forward their views: both sides of the story are important.
Legal language is unavoidable in an AUP. A regulation should only be open to a single interpretation. If you are in doubt about the agreements in this AUP, you can always ask your student councillor or the ICTS Service Desk how to act in a certain situation.

Introduction

Maastricht University (UM, hereinafter: the Institution) offers UM students, visiting and external students, and alumni (hereinafter: Students) the use of various ICT facilities such as Internet connections, equipment and applications (hereinafter: the Facilities). For example, students can use the Internet within the Institution's buildings for study purposes. Students also receive an institution-specific email address, a digital learning environment and other facilities, such as file storage, for personal use in their studies and alumni activities.

The use of the Facilities is subject to rules regarding information security, availability, rights of the Institution and any third parties, and the proper course of business in the Institution's buildings and on its premises. The rules are included in these Student ICT and Internet Regulations (hereinafter: the Regulations). These rules apply to the Institution's students and visiting students. Our aim is to achieve a good balance between student privacy and the responsible and safe use of ICT and the Internet.

To verify that the Facilities are not used in a manner contrary to the rules or applicable laws, and to ensure that the network, equipment and applications are always secure and not overloaded, the Institution may monitor the use of the Facilities as described in these Regulations.

These regulations were adopted by the Executive Board on 17 November 2020. Because the Regulations govern the processing of personal data and monitoring of student behaviour and contain rights and obligations for students, the consent of the University Council of the Institution is required. The University Council agreed to the contents of these Regulations on 22 September 2021.

1. Use of the Facilities

Computer and network facilities (such as public computers, wireless and wired network connections, storage capacity, printers and electronic learning environments) are made available to students for study purposes, including the preparation of assignments, reports and theses, tracking study progress, consulting sources and communicating with lecturers and fellow students.

Students are permitted to use personal equipment and applications on the Institution's Facilities, as long as such use complies with these Regulations. The reconfiguration of equipment and applications made available by the Institution is only permitted with explicit permission from the system administrator. Connecting network equipment for the purpose of sharing the Institution's wired or wireless network connections with others is always prohibited, except in private student living quarters.

These Regulations also apply if you use the network facilities of other Institutions as a guest, gaining access with your own Institution's login details (Eduroam).

Certain Facilities can only be accessed with a username and password, potentially supplemented by an authentication tool such as a smart card or mobile phone. These credentials are personal and may not be shared with others. The system administrator may impose further requirements on password quality and other security aspects, as elaborated in the Information Security Policy. In the event of suspected abuse of a password or means of authentication, the system administrator can immediately disable the account in question.

1.1. Security by the Institution and the student

The institution takes information security seriously. It maintains a strict security policy and takes adequate technical and organisational measures to secure the infrastructure against loss, theft, criminal activities, breach of confidentiality, violation of privacy rights and infringement of intellectual property rights.

However, no security is infallible; the Institution expects students to adopt a proactive attitude and take serious steps to adequately secure personal computers and other equipment (e.g., smartphone or tablet). The Student is always responsible for the use of personal equipment and the data stored on said equipment.

When using personal equipment on a network connection provided by the Institution, students must take the following security measures:

- install an adequate virus scanner and firewall on this equipment;
- prevent unauthorised access to the institution's systems by using hard to guess passwords and/or PIN codes;
- keep the equipment's operating system and software up to date;
- use encryption on the operating system and the stored data.

The UM Information Security Policy and further explanations of security and security measures can be found on the UM security pages: https://www.maastrichtuniversity.nl/informationsecurity.
Specific regulations, agreements or work instructions may apply to specific services and facilities. These will be communicated separately.
If in doubt about agreements, guidelines, measures, etc., please contact the ICTS Service Desk or system administrator.

1.2. Private use and nuisance

Although the Facilities are intended for study purposes, private use is permitted to a limited extent. The use of the facilities (private or for study purposes) must not be illegal or disruptive to the good order of the Institution and must not cause any nuisance to others, infringe the rights of the Institution or third parties or compromise the network integrity and security.

Insofar as use is not part of a study assignment, illegal, disruptive and / or nuisance-causing use is in any case understood:

- publicly accessing Internet services containing pornographic, racist, discriminatory, offensive or objectionable content or sending messages containing such content;
- sending messages with intimidating or sexually harassing content or messages that demonstrate or may incite discrimination, hatred or violence;
- sending messages to large numbers of recipients simultaneously, sending chain letters and phishing emails or distributing malicious software such as viruses, worms, Trojan horses and spyware;
- using file-sharing or streaming services (e.g., Internet radio or video on demand) that generate excessive data traffic to the extent that it may affect the availability of the Facilities;
- downloading films, music, software and other copyrighted material from any illegal source or if the student knows/should know that it violates copyright;
- distributing (uploading) films, music, software and other copyright-protected material to third parties without the rightsholders' consent.

The use of the Facilities for commercial activities is only permitted if the Institution has given its express, written consent.

The use of UM VPN facilities is entirely covered by this AUP, regardless of the network and workstation from which the student started the VPN session.
Students using an Institution’s network facility in their accommodation (e.g., UM Guesthouse locations) will not be restricted in their use there, except to the extent necessary to maintain network integrity and security or limit the effects of congestion. If the institution intervenes to limit the effects of congestion, equal treatment will be given to equal types of traffic. The other provisions of these Regulations apply in full to Students using the Institution’s network facilities in their accommodation.

1.3. Intellectual property and confidential information

Students must not infringe the Institution and third parties' intellectual property rights and must respect the licence agreements in place within the Institution.

Control over the Institution’s information is vested in the Institution. Students have no independent control over the information unless it has been explicitly granted by the Institution.

Students are not allowed to download large quantities of articles from the digital library files or to systematically copy substantial parts of the files or databases in the digital library.

Students who gain access to confidential or privacy-sensitive information during their studies or the performance of tasks for the Institution must treat such information as strictly confidential.

Students must pay particular attention to taking measures, as referred to in these Regulations, if the performance of these tasks necessitates the processing of confidential information outside the Institution, such as by email, in non-institutional cloud applications or on external storage media or personal equipment (USB data carriers, tablets, etc.).
Students must store copies of institution data securely, according to the nature of the data, and make regular back-up copies of these data on the institution’s storage facilities.

If the institution has drawn up further regulations with regard to guaranteeing confidentiality and intellectual property rights, Students are required to follow these promptly.

2. Compliance monitoring by the Institution

The Institution will monitor compliance with these Regulations. The Institution will act within the applicable laws and regulations in monitoring the use of the Facilities.

As part of the monitoring and enforcement of these Regulations, the Institution endeavours to restrict access to individual privacy-sensitive student information or personal data as much as possible, striking the right balance between the responsible use of the Facilities and the protection of students' privacy. The Institution will carry out automated monitoring or filtering as much as possible, without providing insight into individual behaviour to itself or any other person.

2.1. Conditions for monitoring

Monitoring of the use of the Facilities will only take place within the context of enforcing the rules laid down in these Regulations to maintain good order within the Institution and ensure the integrity and security of the Institution's network and computer facilities and the students, staff and third parties.
Technical measures will be implemented to prevent unauthorised use of the Facilities as much as possible.

To this end, automated data are collected (logged). In principle, monitoring will take place at the level of aggregated data, which cannot be traced back to identifiable persons. The data resulting from such monitoring will only be accessible to the system administrators directly responsible and will only be made available to other administrators and managers anonymously. They may decide on further technical measures, such as blocking access to a particular service or restricting network access for the device in question.

In particular, network access can be switched off in the event of nuisance caused by student equipment. The student will be warned in advance, if possible, to allow them to end the nuisance. If this is not possible because of the urgency required, the student will be informed as soon as possible after taking the measure.

In the event of suspected infringement of the rules, targeted investigations may be carried out on the use of the Facilities at the level of individual traffic data for a fixed, short period. The content will only be monitored if there are compelling reasons to do so. The targeted investigation procedure is described in section 2.3 below.

When monitoring traffic data or content, the Institution fully complies with the General Data Protection Regulation (GDPR) and other relevant laws and regulations. In particular, the institution will protect the data recorded during monitoring against unauthorised access, and people with access to the data will be contractually bound to secrecy.

Personal data recorded for supervision and monitoring purposes will be kept for the shortest possible period. This period can only be extended if there is a reasonable suspicion of wrongful use. If an investigation does not lead to any action against a data subject upon completion, the data will be deleted.

2.2. Execution of monitoring

The institution may take specific measures to ensure compliance with these Regulations.
Monitoring for leaks of confidential information—to which the student has access in the context of

their studies or carrying out tasks for the Institution—takes place based on random content filtering. Suspicious messages are flagged for further investigation.

In the context of cost and capacity control, monitoring will also be limited to checking the sources of cost or capacity demand (such as the addresses of Internet radio and video sites) through traffic data. If these websites lead to high costs or nuisance, they will be blocked or cut off, without violating the confidentiality of the content of the communication;

The ICT department and the system administrators are bound by confidentiality if, in the context of monitoring these Regulations, they must obtain personal information for technical reasons, unless any legal requirement or the completion of their work obliges them to disclose it.

In the context of monitoring for compliance with these Regulations, the Institution will take the necessary measures to ensure that personal data are accurate and correct in relation to the purposes for which they are processed.

In the context of monitoring for compliance with these Regulations, the Institution will take appropriate technical and organisational measures to protect personal data against loss and any form of unlawful processing.

2.3. Targeted investigation procedure

A targeted investigation involves recording traffic data or other personal data concerning the student within the framework of an investigation following a serious suspicion of a violation of these Regulations by that student.

A targeted investigation will only take place after written instruction from the Executive Board. The instructions must also specify who will be informed of the investigation and, if necessary, the recorded results. If the investigation does not give rise to any further action, the records will be destroyed.

A targeted investigation is initially limited to traffic data on the use of the Facilities. If a targeted investigation provides further evidence, the Institution may follow a separate instruction from the Executive Board and examine the content of communications or stored files. If the investigation does not give rise to any further action, the records will be destroyed.

In deviation from the above, targeted investigations into the security or integrity of peripherals may be carried out by the system management based on concrete indications, without separate authorisation. The results of such investigations are only shared with the student to improve the security or integrity of peripherals. The procedure set out in the previous two paragraphs will be followed for repeated infringements.

The student will be notified of the reason, the execution and the result of the investigation in writing on behalf of the Executive Board as soon as possible. The student will be allowed to explain the data found. Notification may only be delayed if it would harm the investigation or is very likely to do so.

System administrators may only access the student’s accounts or computers with the student’s consent. Access to accounts without such consent is only permitted in urgent cases or where there is a clear suspicion of a breach of these Regulations, as specified in this article. In that case, the student will be notified afterwards.

3. Consequences of violation of these Regulations

In the event of a violation of these Regulations or generally applicable legislation in the use of the Facilities, the Executive Board may take measures, depending on the nature and seriousness of the violation.

Such measures may include a warning, reprimand, temporary disqualification or restriction of the Facilities (maximum of one year) and, in extreme cases, termination of enrolment as a student.

Measures (other than a warning) cannot be taken solely based on automated processing of personal data, such as detection by an automatic filter or blockade. In the event of a warning based on automated processing, the student will be allowed to present their views. Furthermore, no measures are taken other than in the event of repetition of facts as described in the following paragraph.

Temporary or permanent restrictions on access to certain Facilities or other measures of order may be imposed if an action is taken in violation of these Regulations and a prior warning has been issued setting out the nature of the actions observed and the consequences of a possible recurrence. The student will first be allowed to present their views in response to the aforementioned warning.

Contrary to the above, in the event of (automated) detection of nuisance, the institution may temporarily block the facility in question. This blockade will be maintained for a maximum of one week or shorter if the cause has been satisfactorily eliminated. If the system administrator has noted no improvement after one week, they may decide to extend the blockade. In the case of repeated infractions, additional measures may be taken.

If any of the offences found to have been committed are covered by the Computer Crime Act, the institution will file a police report.

4. Student rights regarding personal data

The student has all the rights regarding personal data processing under the GDPR, as laid down in the UM privacy statement.

The student is also entitled to a human assessment of decisions based on automatically processed data.

5. Final provisions

These Regulations may be revised by the Executive Board. Changes should preferably be made at the beginning of a formal study period (September or February), except in urgent cases or when external circumstances force the Institution to set an interim or deviating implementation date. In all cases, students must be informed in good time.

Changes will only be made after the University Council has been asked for its advice. The Executive Board will consider feedback from students before making the changes.

In cases not provided for in these Regulations, the Executive Board will decide.

Adopted by the Executive Board of Maastricht University on: 17 November 2020
Approved by the University Council on: 22 September 2021

Source reference:

The ICT regulations for UM staff and students are based on the Model Regulations for Higher Education, drawn up by the SURF Community for Information Security and Privacy (SCIPR: www.scipr.nl) and published under the Creative Commons 4.0 license.