Acceptable Use Policy

Acceptable Use Policy (AUP) for students studying at Universiteit Maastricht

The Universiteit Maastricht (hereinafter referred to as: the Institution) offers its own students, extraneï and alumni (hereinafter referred to as: students) and visiting students the opportunity to use the Internet for study purposes and alumni activities. An institution-related mailbox and options for storing files and personal study information will also be made available for personal use by students for study purposes and alumni activities.
Rules are attached to the use of these facilities to ensure the smooth course of events in the buildings and on the Institution's grounds.

1. Use of the 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) will be made available to students and alumni for the purpose of study to enable the student to carry out assignments, prepare reports and theses, keep a record of study progress, consult sources of reference and communicate with lecturers and fellow students, participate in alumni activities among other things.
The use of personal equipment and applications on the Institution's facilities as allowed, provided such use is in accordance with the rules set out in these Regulations. Changing the settings of equipment and applications made available by the Institution is only permitted with the explicit consent of the Institutions (local) IT-support. Connecting personal network equipment for the purpose of sharing the connection with third parties on wired or wireless network connections is prohibited at all times.
These Regulations also apply to guest access at other institutions, making use of credentials of one's own Institution (Eduroam).
Certain facilities will only be accessible with the aid of a username and password or by other means of authentication, such as a smartcard or GSM. These are person-related and are not permitted to be shared with other persons. In the event of suspected misuse of a password or other means of authentication, (local) IT-support may block access to the relevant account with immediate effect.
UM's Information Security Policy and additional information on information security and applicable guidelines are available on UM's security pages:
http://www.maastrichtuniversity.nl/informationsecurity.
Specific IT-services or facilities may be subjected to specific regulations or guidelines, which will be communicated separately. In any case of doubt regarding this AUP one should contact Servicedesk ICTS or the department's local IT-support.

2. Intellectual property and confidential information

The student will not infringe on intellectual property rights of the Institution or third parties and will respect applicable Licence agreements. Property rights on information from the Institution will be solely controlled by the Institution. The student will only be eligible for property rights on such information if those rights are explicitly granted by the Institution.

If the student gets access to confidential or privacy sensitive information in order to fulfill assignments for the Institution, the student is obliged to maintain confidentiality of this information at any time.

The student will pay special attention to implementing security measures as stated in paragraph 3 of this document if an assignment makes it necessary to transfer confidential information outside the control of the Institution, for example through sending it by e-mail or storing it on non-Institutional Cloud-services, external media or student owned devices (USB devices, Tablets, etc.)
If the Institution has issued specific instructions to safeguard confidentiality and protection of intellectual property, the student is obliged to adhere to these instructions strictly.

3. Security policy for the Institution ánd the student

The Institution takes information security seriously. The Institution therefore maintains a stringent security policy and takes proper technical and organisational measures to protect the infrastructure against loss, theft, criminal activities, loss of confidentiality, privacy breaches and infringements on intellectual property rights.
It obviously is impossible to ensure one hundred per cent security. For this reason the Institution expects students to adopt a proactive approach and take serious measures to secure their own computer and other equipment, such as smartphones or tablets, properly.
Students are at all times personally responsible for the use of their own equipment and for the data stored on the equipment.
If students use their own equipment on the Institution's facilities, they should ensure the following security measures in particular:

- their equipment features an effective protection against viruses and other malware[1] and a firewall;
- they should regularly make back-ups of all relevant data and store copies of Institution data securely;
- use passwords that are difficult to decipher and change these on a regular basis;
- keep the software settings on their equipment up-to-date;

UM's Information Security Policy and additional information on information security and applicable guidelines are available on UM's security pages:
http://www.maastrichtuniversity.nl/informationsecurity.

4. Personal use and disturbance

The Institution offers ICT-facilities to students to perform study related activities. Limited personal use of the facilities is permitted, however the activities must not disturb good order in the Institution and must not cause disturbance to others, cause an infringement on the rights of the Institution or others, nor be detrimental to the integrity and security of the network.
Use causing interference and/or disturbance is always taken to mean the following:

- consulting Internet services that have a pornographic, racist, discriminatory, insulting or offensive content in public spaces or sending messages with such content;
- sending harassing/sexually harassing messages or messages that incite or could incite discrimination, hatred and/or violence;

[1] Malware: malicious software e.g. Trojan Horses, Worms, Viruses, Spyware , etc.

- sending unsolicited messages to vast numbers of recipients, sending chain letters or sending malware, such as viruses, worms, Trojan horses and spyware;
- using file sharing or streaming services (such as Internet radio or TV-on-demand) if the volume of data traffic imposes a threat to the integrity and safety of the computer or network facilities;
- downloading films, music, software and other copyright-protected material from any illegal source or if the student actually knows that this violates copyrights;
- distributing or uploading films, music, software and other copyright-protected material to or for third parties without the consent of the owners.

These Regulations also apply to the use of UM's VPN[2] facilities, regardless of the network or the workstation the student uses to initiate the VPN session.
No restrictions will be imposed on use by students using an Institution network facility in their living accommodation (e.g. an UM Guesthouse location), except where required to ensure the integrity and security of the network, or to guarantee network availability. If the Institution intervenes in order maintain to network availability, the same types of traffic will be treated equally. The other provisions set out in this Acceptable Use Policy apply in full to student users using an Institution network facility in their living accommodation.
Use of the Institutions computer and network facilities for the purpose of performing commercial activities is solely permitted if and to the extent the Institution has provided written consent to do so.

5. Monitoring and investigations by the Institution

Monitoring the use of facilities will only be carried by the Institutions IT-support to enforce the rules set out in these Regulations for the purpose of ensuring good order at the Institution and to monitor the integrity and security of the Institution's network and computer facilities. Use of the facilities for purposes designated as prohibited will be rendered impossible by means of technical solutions as far as possible.
To monitor compliance with the rules, information will be collected on a computerised basis (logged). Only the Institutions IT-support in charge will have access to the information, which will only be made available to other IT-support staff and officers in charge in an anonymised format. They may decide to take further technical measures, such as blocking access to a certain service or limiting the options on the relevant equipment in order to use the network.
Switching off the network access options is a special measure that may be taken in the event of disturbance caused by students' own equipment. The student will receive an advance warning, if possible, offering him or her opportunity to stop causing disturbance. If it is not possible to warn the student in advance of taking the measure due to the required urgency, the student will be notified of the measure as soon as possible.

If there is reason to believe that these Regulations have been violated or the smooth course of events in the buildings and on the Institution's grounds have been put at risk, monitoring may be performed at the level of individual traffic data relating to use of the facilities. Only if there are important reasons for doing so will the content be investigated.
Such a specific investigation will be conducted only after the Executive Board (CvB) or a mandated dean or director has commissioned the investigation in writing. The CvB will receive a copy of the

[2] VPN: Virtual Private Network: a safe way to connect a workstation to the Institutions network through Internet

order commissioning the investigation and a document containing the results of the investigation. If no further measures are required as a result of the investigation, the document will be destroyed.
The student will be informed by the mandated director in writing of the reason for conducting the investigation, the procedure and the results as soon as possible. The student will be given the opportunity to explain the findings. Informing the student may only be postponed if this would actually be detrimental to the investigation.
Mandated Institutions IT-support staff will only provide access to student accounts or information if the student has given consent to do so. Access without the student's consent is only permitted in urgent cases or if there is a clear suspicion that these Regulations have been violated, as detailed in this Article. In such case the student will be informed at a later stage.

When performing a check at the level of traffic data or content, the Institution will fully abide by the Data Protection Act and other relevant laws and regulations. The Institution will specifically protect the data recorded during the check against unauthorised access while persons having access to the data will be bound by contract to maintain confidentiality thereof.

All Institutions IT-support staff members are submitted to the work instructions in the "Integrity and behaviour code for ICT staff at UM" <version 3.1 formalized by UM's CBB dd.: 26-09-2006>.

6. Student privacy rights

The student may request the Board for a complete overview of his or her personal data as processed by the Institution for the purpose of these Regulations. A request of this nature will be complied with within four weeks.
The student may request the Board to improve, add to, remove or protect his or her personal data if they are factually incorrect, incomplete for the purpose in mind or irrelevant, or conflict with statutory provisions. A request of this nature will be complied with within four weeks. A refusal will be accompanied by reasons. A request that has been granted will be carried out as soon as possible.
The student may also lodge an objection against the processing of his or her personal data on the grounds of serious personal circumstances. The Board will decide whether the objection is justified within four weeks of receipt. If the Board deems the objection justified, it will stop processing the data with immediate effect.

7. Consequences of violation

The Executive Board may take disciplinary measures in the event a student acts in contravention of these Regulations, depending on the nature and seriousness of the violation.
This includes a warning, reprimand, temporarily blocking or limiting the facilities (for a maximum period of one year) and in extreme cases termination of the student's enrolment, as regulated in Dutch laws on Higher Education (WHW: Wet op het Hoger onderwijs en Wetenschappelijk onderzoek).
Disciplinary measures, except for a warning, may not be taken solely on the basis of computerised processing of personal data, such as a finding generated by an automatic filter or block. In addition, no disciplinary measures will be taken without giving the student the opportunity to state his or her views.

Specific measures limiting the use of ICT-facilities, whether or not temporarily, or other disciplinary measures can be taken by the Institution in the event of recurrent student actions in contravention of these Regulations after a prior warning has been issued to the student, stating the type of the offence on record and the consequences of recurring offences of this type.

Contrary to the above, it is possible for the Institution to temporarily block the relevant facility in the event disturbance is detected by the computer or otherwise. The block will be maintained for a maximum period of one week or shorter if the cause has been removed to the satisfaction of the Institutions IT-support staff. If IT-support establishes after one week that no improvement has been made, IT-support may decide to prolong the block.

8. Concluding provisions

These regulations may be amended by the Executive Board. Amendments will preferably be implemented at the start of an academic period, except in urgent cases or if external circumstances dictate that the Institution should do so earlier. In all cases students will be informed timely regarding these amendments.
Amendments will only be implemented after a prior opinion has been sought from the University Council (Univeristeitsraad). The Executive Board will consider student feedback before implementing the amendments.

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

Approved and adopted by the Executive Board on 17 June 2013
Adopted by The University Council on 25 September 2013