Acceptable Use Policy

UM Employee ICT and Internet Regulations.

Version 2.0

17 November 2020

Version	Status	Date	By
1.1	Concept	27 July 2020	CISO
1.2	Concept	20 August 2020	Privacy Team / UM-SOC
1.3	Approval	30 June 2021	Employee Representation
2.0	Adoption	17 November 2020	Executive Board

Table of Contents

Acceptable Use Policy 1

UM Employee ICT and Internet Regulations. 1

Preamble 3

1. Introduction 4

2. General 5

Article 1. Purpose 5
Article 2. Scope 5

3. Code of Conduct 6

Article 3. Use of the Facilities 6
Article 4. Use of email and other electronic communication 6
Article 5. Use of Internet 7
Article 6. Bring your own device (BYOD) 7
Article 7. Private use of the Facilities 8
Article 8. Use of social media 8
Article 9. Intellectual property and confidential information 9

4. Compliance monitoring and measures 10

Article 10. Conditions for monitoring 10
Article 11. Execution of monitoring 10
Article 12. Targeted investigation procedure 11
Article 13. Consequences of violation 12
Article 14. Employee rights regarding personal data 12
Article 15. Final provisions 13

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 employees. An AUP is necessary to make it clear to employees how they can use UM's ICT facilities to perform their duties, 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 an employee will be respected.
Therefore, this AUP is available to every employee. 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 local IT support, your Information Manager, your manager or the ICTS Service Desk how to act in a certain situation.

1. Introduction

The use of network facilities and ICT resources (hereinafter: the Facilities), is necessary for employees at Maastricht University (hereinafter: the Institution), to perform their work properly. However, there are risks associated with such use, necessitating the establishment of rules of conduct. Employees may be expected to use the Facilities responsibly in light of these risks. With these ICT and Internet Regulations (hereinafter: the Regulations), the Institution wishes to lay down rules regarding the desired use of the Facilities. Our aim is to achieve a good balance between employee privacy and the responsible and safe use of ICT and the Internet.

The use of social media such as Facebook, LinkedIn, WhatsApp and Twitter has become indispensable but can also have repercussions for the Institution. To prevent such repercussions, the Institution wants to lay down certain rules governing such use, detailed in these Regulations.

Pursuant to Article 7: 660 of the Dutch Civil Code, the Institution as an employer is authorized to set rules about the performance of the work and good order in the workplace.

The Executive Board adopted these regulations on 17 November 2020. Because the Regulations govern the processing of personal data and monitoring of employee behaviour and contain rights and obligations for employees, the consent of the Institution's University Council and Employee Representation is required. The University Council and the Local Consultative Body agreed to the content of these Regulations on 22 September 2021 and 30 June 2021, respectively.

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 there is any doubt about agreements, guidelines, measures, etc., the manager can explain.

2. General

These Regulations for ICT and Internet Use by Employees of the Institution specify the agreements regarding various topics relating to the use of Facilities and their effect on employees in daily practice. The purpose of these Regulations and their applicability are set out below.

Article 1. Purpose

The Regulations lay down rules regarding the use of company ICT and Internet resources by employees. The rules are aimed at establishing good order with regard to:

- system and network security, including protection against damage and abuse;
- combating sexual harassment, discrimination and other illegal activities;
- protection of the Institution's privacy-sensitive information, including the personal data of its employees, (former)students and other parties involved;
- protection of the confidential information of the institution and its employees, as well as students and parents;
- protection of the Institution and third parties' intellectual property rights, including compliance with the licensing agreements applicable within the Institution;
- prevention of negative publicity;
- cost and capacity management.

Article 2. Scope

2.1. These Regulations apply to everyone who works for the Institution and uses the Facilities made available by the Institution. The Regulations also apply to temporary employees and self-employed persons, guest lecturers, seconded employees and trainees who have been deployed to carry out work for the Institution. These Regulations also apply to guests of employees.
The Regulations do not apply to students; separate Student Regulations have been drawn up for this purpose. "https://www.maastrichtuniversity.nl/informationsecurity"

2.2. 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).

2.3. These Regulations will be issued to everyone working for the Institution on commencement of appointment, and employees will be informed of where to find the latest version.

2.4. Guests are reminded of these Regulations when they are granted access to the guest network and can save them if desired.

2.5. The use of UM VPN[1] facilities is entirely covered by this AUP, regardless of the network and workstation from which the employee started the VPN session.

[1] VPN: Virtual Private Network: A secure way to connect a workstation to the institution's network via the Internet

3. Code of Conduct

The Institution makes Facilities available to everyone working for it, for the performance of their duties. This chapter sets out the agreements to which everyone working for the Institution must adhere when using those Facilities. The institution also expects employees to take responsibility for the correct use of the resources made available.

Article 3. Use of the Facilities

3.1. The employee will be issued personal login details (username and password) and any other means of authentication necessary to access the Institution's Facilities (e.g., smart card or token). The employee must always handle login details and any other means of authentication with care. Personal passwords and other means of authentication may not be shared. In the event of suspected abuse of a password, the system administrator can immediately disable the account involved.

3.2. The Institution may prescribe systems or applications for educational and other business purposes, such as an electronic learning environment, an email system, mobile applications (apps), cloud facilities or multimedia services. Employees may only use these prescribed systems to provide education or to conduct research, observing strict compliance with the relevant restrictions and requirements.

3.3. Installing software on the ICT facilities and using the network facilities of the organization is only allowed as far as rights to be granted to the user. Connecting servers and active network components (e.g., access points and routers) is not permitted without the system administrator's permission.

3.4. The use of the Institution's facilities through other networks or from home is only permitted via secure (Wi-Fi) networks and the secure access made available for this purpose (e.g., VPN or virtual desktop) using the Institution's equipment or using personal equipment, provided that such equipment meets additional requirements, such as installing virus scanners, regularly updating the operating system, and using encryption and password protection. Further explanations of security measures can be found on the UM security pages: https://www.maastrichtuniversity.nl/informationsecurity.

3.5. The Facilities may only be used for ancillary activities with the Institution's express, written consent.

3.6. The employee may process personal data in the performance of the work assigned to them. All processing of personal data carried out by the employee in the context of their work, using the Institution's Facilities (including prescribed systems or applications) or otherwise, must comply with the requirements under the GDPR and must fit in with their regular work. For more information, see the UM privacy policy on the UM Privacy page.

Article 4. Use of email and other electronic communication

4.1. The email system and the associated mailbox and email address are made available to the employee for use in their work. The use of these resources is limited to tasks arising from such work. The use of these resources for private purposes or ancillary activities is only be permitted as stipulated in Article 7.

4.2. Employees are only permitted—within the performance of the work assigned to them—to send personal data from the Institution by email and other ICT means if it is part of their regular work and has been tested for compliance with the GDPR.

4.3. The following use of electronic communication, except for specific, job-related tasks, is prohibited in any case:
- sending messages containing pornographic, racist, discriminatory, threatening, insulting or offensive content;
- sending messages with intimidating or sexually harassing content;
- sending messages that incite, or could incite, discrimination, hatred or violence;
- sending unsolicited messages to large numbers of recipients, chain letters and phishing emails or sending malicious software such as viruses, Trojans or spyware.

4.4. In the event of illness, unexpected, prolonged absence or gross negligence on the part of the employee, and only if it constitutes a reason for access due to compelling business interests, the Institution is entitled to provide a replacement with access to the employee's files or mailbox. This is only applicable if (i) it can be demonstrated that it is impossible to obtain permission from the employee or that the company's interests are such that permission cannot be required, and (ii) separate permission has been obtained from the Executive Board. However, the Institution may not access folders marked as private, emails recognisable as private, or emails sent to or from a confidential counsellor, ombudsman, (members of an) employee participation body[2] or Local Consultative Body, company doctor, HR adviser or Labour Union adviser. If the employee has not applied such markings, the institution shall use a confidential adviser to check such information to identify and separate private information before the replacement is granted access.

Article 5. Use of Internet

5.1. Internet access and associated facilities are made available to the employee for use in their work. The use of these resources is limited to tasks arising from such work. The use of these resources for private purposes or ancillary activities is only be permitted as stipulated in Article 7.

5.2. Employees are only permitted—within the performance of the work assigned to them—to process personal data from the Institution on the Internet if it is part of their regular work and has been tested for compliance with the GDPR.

5.3. The following use of the Internet, except for specific, job-related tasks, is prohibited in any case:
- visiting sites that contain pornographic, racist, discriminatory, abusive or offensive material;
- 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 employee has reasonable grounds to believe that it violates copyright;
- distributing (uploading) films, music, software and other copyright-protected material to third parties without the rightsholders' consent.

Article 6. Bring your own device (BYOD)

6.1. Anyone working for the Institution is permitted to use personal equipment for this purpose, provided that such equipment meets the security requirements set out below. Certain highly sensitive activities, such as system administration, may be subject to specific agreements prohibiting the use of personal equipment.

6.2. Employees are only permitted to connect private equipment (e.g., laptops, tablets and telephones) to the network connections provided for this purpose. The system administrator

[2] University Council, faculty and service councils, etc.

may place rules on access through these connections to enforce these regulations, such as installing virus scanners, regularly updating the operating system, and using encryption and password protection.

6.3. Anyone using personal equipment to perform work for the Institution is responsible for taking appropriate security measures. Employees are expected to take at least the following security measures:

- Secure the device with a strong password or PIN;
- lock the device when leaving the workplace;
- do not use personal devices to store personal data for which the Institution is responsible; this is not permitted;
- encrypt all data relating to the Institution if, for any reason, it is not stored on the Institution's network (e.g., a personal device or USB stick);
- keep (encrypted) data from the Institution and private data separated. This separation must be clearly recognisable on the personal device;
- keep software up to date by performing periodic updates (at least monthly);
- take adequate measures against viruses or malware by keeping the virus scanner up-to-date and scanning the device periodically (at least monthly).

Further explanations of security measures can be found on the UM security pages: https://www.maastrichtuniversity.nl/informationsecurity.

Article 7. Private use of the Facilities

7.1. The Facilities are made available to the employee for use in the context of their work. The use of these resources is limited to tasks arising from such work.

7.2. Private use of the Facilities is permitted to a limited extent, provided it is not disruptive to day-to-day operations, good order in the workplace or the Institution's network.

7.3. The storage of private files or information on the Institution's systems is permitted, provided that it does not lead to an overload of the Institution's network or the storage capacity of these systems. However, the institution is not obliged to make back-ups of such files or information or make copies available in the event of replacement or repair of the systems concerned.

7.4. The employee should not use the email address provided by the Institution for personal communication, if possible. The organisation will not block or specifically monitor access to other email services.

7.5. Occasional personal use of the mobile phone provided by the Institution abroad is permitted.

7.6. Occasional personal use of a mobile network while abroad (roaming) is permitted.

Article 8. Use of social media

8.1. Social media (e.g., Facebook, YouTube, Instagram, Skype, WhatsApp, Twitter or LinkedIn) is permitted for matters involving the employee's position or performance. However, the employee must take care not to harm the good name of the Institution and anyone involved. In other words, social media must be used responsibly[3].

8.2. The Institution supports open dialogue, exchanging ideas, and sharing the employee's knowledge with peers and third parties through social media (e.g., Facebook, YouTube, Instagram, Skype, Twitter or LinkedIn).

[3] See also the guidelines on the use of social media:
https://www.maastrichtuniversity.nl/support/communications-guide/social-media

For work-related topics, the employee must ensure that the profile and content align with how they would present themself to colleagues and students in text, images and sound.

8.3. Directors, managers, executives and others who promote policy or strategy on behalf of the Institution have a special responsibility when using social media, even if the content is not directly related to their work. Based on their position, they must consider whether they can publish in a personal capacity. They need to be aware that employees read what they write.

8.4. Sharing or distributing other people's personal data through social media in a professional capacity is only permitted if it fits in with the employee's regular work and has been tested for compliance with the GDPR. Extra attention should be paid to the distribution of visual material (photos and videos) in which others can be identified; this usually requires the explicit consent of those concerned.

8.5. This article also applies to employees' use of social media from personal computers or Internet connections, but only to the extent that such use may affect their work.

8.6. If an employee sets up a work-related social media account in their own name, the employee and the Institution will seek an appropriate solution for transferring the profile or the information and contacts it contains in the event of employment termination.

Article 9. Intellectual property and confidential information

9.1. The employee must treat confidential information and privacy-sensitive information—including personal data—to which they have access in the context of their work, as strictly confidential and take sufficient measures to ensure confidentiality.[4]

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

9.3. Control over the Institution's information is vested in the Institution. The employee has no independent control over the information unless the Institution has explicitly granted it.

9.4. The employee is not permitted 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.

9.5. The employee must pay particular attention to taking measures, as referred to in these Regulations, if the performance of their work 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 sticks, tablets, etc.). The employee must strictly comply with any regulations drawn up by the Institution with regard to confidentiality, GDPR compliance and the protection of intellectual property.

9.6. These provisions will apply in particular to system administrators, for whom a breach of these provisions will be considered a serious breach of duty in light of their special position.

[4] This confidentiality applies without prejudice to the provisions of the Maastricht University Regulations on Reporting Misconduct (Regeling Melding Misstanden Universiteit Maastricht).

4. Compliance monitoring and measures

This chapter outlines how the Institution monitors compliance with these Regulations and what action may be taken if the Regulations are breached.

The Institution will act within the applicable laws and regulations in monitoring the use of the Facilities it makes available for the performance of the employee's work.

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

Article 10. Conditions for monitoring

10.1. The use of the Facilities will only be monitored within the context of enforcing these Regulations for the purposes referred to in Article 1. Technical measures will be implemented to prevent unauthorised use of the Facilities as much as possible.

10.2. Data is collected (logged) automatically for monitoring compliance with the rules. In general, 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.

10.3. In the event of suspected infringement of the rules, targeted investigations may be carried out on the use of the Facilities—such as email and Internet usage—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 will be conducted, as described in Article 12.

10.4. 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.

10.5. 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.

Article 11. Execution of monitoring

11.1. Some specific (and preferably automated) measures the Institution may take include:

- measures to prevent negative publicity and sexual harassment and measures in the context of system and network security, will be based on keyword filtering, also known as content filtering. Suspicious messages are automatically returned to the sender or refused, deleted or flagged for further investigation;

- In the context of cost and capacity control, monitoring will 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;

- visual material is monitored based on third-party complaints or reports, or randomly in the case of visual material that is publicly available;
- the systems will be monitored for internal and confidential data leaks based on random content filtering. Suspicious messages are flagged for further investigation in consultation with the board.

11.2. IT staff and system administrators are bound by confidentiality if, in the context of the monitoring of 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.

11.3. System administrators may only access employee accounts or UM-managed employee equipment with the employee's consent. Access to such accounts or equipment without employee's consent is only permitted in urgent cases or where there is a clear suspicion of a breach of these Regulations, as specified in Article 12. In that case, the employee will be notified afterwards.

11.4. 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.

11.5. 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.

Article 12. Targeted investigation procedure

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

12.2. A targeted investigation will only take place after written instruction from the Executive Board. The instructions will also include 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.

12.3. Contrary to the previous paragraph, a targeted investigation of the security or integrity of equipment will be carried out by the system administrator based on specific information. In that case, separate permission from the board as referred to in paragraph 2 is not required. The results of such investigations are only shared with the employee to improve the security or integrity of equipment. The procedure set out in paragraph 2 will be followed for repeated infringements.

12.4. 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 examine the content of communications or stored files. Such examination requires a written instruction from the Executive Board, which must include why it is given. The institution will make every effort to obscure the identity of the people carrying out the examination. The examination will be conducted in the name of the Executive Board.

12.5. Emails sent to or from (members of) employee participation bodies[5] or the Local Consultative Body, a company doctor, a confidential counsellor or an ombudsman, HR or labour union consultants and anyone who may invoke confidentiality under the law, will not be examined. This does not apply to automated monitoring of the security of email traffic and the network.

[5] University Council, faculty and service councils, etc.

12.6. Assessments of violation of Articles 4(3) and 5(3) will be conducted by two people, based on a serious suspicion, by opening emails or files and consulting their contents (preferably by random sampling). These people have been appointed for this purpose by the Executive Board[6] and are bound to confidentiality with regard to the content.

12.7. The employee 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 employee will be allowed to explain the data found. Notification may only be delayed if it would harm the investigation or is highly likely to do so.

Article 13. Consequences of violation

13.1. When acting contrary to these Regulations or the generally applicable statutory rules, the board can take appropriate measures, depending on the nature and seriousness of the violation. In addition, the board can decide to limit, temporarily or otherwise, access to certain ICT facilities.

13.2. 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 employee will be allowed to present their views. Furthermore, no measures will be taken other than in the event of repetition of established facts in accordance with Article 13.3.

13.3. The Institution may impose temporary or permanent restrictions on access to certain ICT facilities and other measures 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 employee will first be allowed to present their views in response to the aforementioned warning.

13.4. In addition to the above, in the event of (automated) detection of nuisance, the institution may temporarily block the facility in question. The blockade will be maintained until it has been demonstrated that the cause has been removed. In the case of repeated infractions, measures may be taken.

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

Article 14. Employee rights regarding personal data

14.1. The employee has all the rights regarding personal data processing under the GDPR, as laid down in the UM Employee https://intranet.maastrichtuniversity.nl/en/um-employees-privacy-statement (Intranet).

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

14.3. The board will not issue instructions or service orders to the employee regarding privacy-sensitive information and personal data in contravention of these Regulations.

[6] They are usually members of the UM Security Operations Center (UM-SOC) or the UM Privacy Team.

Article 15. Final provisions

15.1. These Regulations are evaluated by the Executive Board every year.

15.2. The organisation may amend these Regulations if circumstances so require, with the consent of employee participation bodies and the Local Consultative Body, where applicable. Proposed changes will be announced to employees before implementation. The board will consider employee feedback before implementing the changes.

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

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.