Wageningen University (WU) – Network Regulations Governing Students (2022)

Summary

Wageningen University offers students the opportunity to use network facilities, equipment, software and data (hereinafter referred to jointly as the 'Facilities'). As such, students have the opportunity to use the internet for their studies within our buildings and in the student residences on campus. Students are also provided with a personal mailbox and access to an electronic learning environment for their studies.

These regulations govern the use of our Facilities by WU and visiting students, such as guest and exchange students. In the case of students who are also WU staff members, the network regulations for staff members and other personnel also apply, hence both sets of regulations. In this case, the capacity in which the Facilities are used will determine which regulations are applicable.

When logging in with a new account or when an amended version of these regulations is adopted by the Executive Board, everyone will be given an opportunity to familiarise themselves with the content of these regulations by means of a pop-up window when logging in for the first time. Students will then be required to declare their consent before they can log in. Students will also have their attention drawn to the place where they may find the applicable version of these network regulations.

What is acceptable use of the Facilities?

Whenever you use the Facilities that we provide to you for the purposes of your studies, you are required to comply with the WU code of conduct in relation to data security, accessibility, our rights and those of any other parties, and appropriate conduct in our buildings and on our grounds. This code of conduct has been incorporated into these regulations.

The following principles apply with regard to any use:

I) The Facilities will not be used for any activity in breach of the applicable legislation or public decency.
II) The Facilities will not be used for any activities that are harmful, pose a threat or are offensive to any other party.
III) The use of the Facilities will not compromise their availability, integrity or confidentiality (including any data held in them).

These principles are set out in greater detail as concrete codes of conduct in these regulations, for example, for security and the prevention of nuisance.

How does WUR monitor the use and security of the Facilities?

In order to check that the Facilities are not used in a way contrary to the provisions of these rules or the applicable legislation and regulations, and to ensure that the Facilities and the information within them is secure and not overloaded at all times, we may monitor the use of the Facilities in the manner set out in these regulations. In this respect, we seek to achieve a healthy balance between the responsible and secure use of the Facilities and students' privacy. For this reason, we ensure that any

monitoring conducted by us or on our behalf is proportional: the greater the risks and the more specific the indications of a breach, the more far-reaching and focused the monitoring may be.

General monitoring

In the first instance, monitoring occurs automatically at the level of aggregated data. This means that data is monitored generally in such an aggregated way that it produces an overall picture of the use of all or part of the Facilities. Data that is traceable to individuals is only consulted if an automated alert constitutes grounds for doing so.

In addition to general monitoring that occurs on the basis of aggregated data, information that can be traced back to individual users is collected in the case of specific forms of general monitoring, such as mobile device management and simulated attacks on networks and/or systems. Such data is only used for the purposes for which it is collected, namely verifying compliance with and the enforcement of these regulations. The data is deleted once it is no longer required for that purpose.

Focused investigation

Focused investigation occurs where the data of a specific student is recorded because there is a compelling suspicion that they have contravened these regulations. For example, we may inspect the content of any communication or file check whether there has been an actual breach.

What are the implications of breaching these regulations?

Where it is necessary to avoid damage, the use of all or part of the Facilities may be blocked immediately. Should we detect a breach of these regulations, the student concerned will have an opportunity to explain their position before any move is made to adopt disciplinary measures. In addition to disciplinary measures, we may press charges in the case of a criminal offence and/or recover any losses that have been incurred because of the culprit.

How is students' privacy protected?

When enforcing these regulations, we comply with the applicable legislation and regulations, including the General Data Protection Regulation (GDPR). The personal data that we retain in response to any general monitoring or targeted investigation is secured appropriately. Only staff members who need to have access to such personal data – a very limited group – have access to it. An attempt will always be made to collect as little personal data as possible to achieve the goals of these regulations. In cases in which we process personal data, as few people as possible will have access to it, and it will be secured appropriately. See this link in relation to these regulations for more information about the students' personal data that we process, and how and why we do this.

Contents

1. Use of the Facilities

We provide you as a student with computer and network facilities (such as public computers, wired and/or wireless network access, storage capacity, printers and electronic learning environments) – hereinafter: the 'Facilities' – for your studies to enable you to carry out assignments, write reports and theses, keep records of your educational progress, consult sources, and communicate with lecturers and your fellow students, amongst other things.

As a student, you may use your own equipment and applications with our Facilities, as long as you comply with the provisions of these regulations when using them, and do not breach the applicable legislation and regulations or social standards of decency. The settings of the equipment and applications that we make available may only be changed with our consent. Connection to students' own network equipment to enable any other party to share our network connections is prohibited at all times.

These regulations also apply if you make use of other organisations' network facilities in your capacity as a guest and you obtain access to them using the login details of your own organisation (Eduroam).

Certain Facilities may only be accessed with the aid of login details. These are personal and you are not intended to share these details with anyone else. We may stipulate additional requirements in terms of the nature of passwords and other security aspects, as set out in greater detail in our Information Security Policy. Where there is any suspicion that a password or other means of authentication has been misused, we may immediately render the relevant account inaccessible.

1.1. Security

We take data security very seriously. As such, we pursue strict security policy and adopt appropriate technical and organisational measures to secure our infrastructure, and WU's and its students' information securely against loss, theft, criminal activities, disclosure and the infringement of privacy and intellectual property rights.

This is a shared interest. It is not only in our interest but also in the interest of the users of the Facilities. This includes you as a student. For this reason, we also expect students to adopt a proactive approach and to take serious steps to ensure that their own computers and other equipment (such as smartphones or tablets) are properly secured. As such, students are themselves responsible for the use of their own equipment and any data stored on it at all times.

In particular, when you utilise our network connection using your own equipment, for the purposes of security you are required to:

- equip this equipment with a good virus scanner and firewall;
- prevent unlawful access to our systems by using strong, unique passwords and/or PIN codes;
- ensure that this equipment is kept up-to-date in terms of software settings;
- use encryption.

The central information security officer (CISO) will publish a list of security measures, which will be revised regularly. We expect you to ensure strict compliance with these measures, which apply in relation to you as a student.

1.2. Personal use and nuisance

Although the Facilities are intended to be used for the purposes of your studies, you may also use them for other purposes to a limited extent. Nevertheless, you need to consider that the Facilities are never used for unlawful purposes or in such a way that they disrupt the good order or occasion nuisance for others. Furthermore, you may not infringe the rights of WU or any other party, nor may you impair the integrity or security of the network.

Any use of the Facilities that is unlawful or disruptive and/or occasions nuisance is at any rate deemed to refer to:

- accessing internet services in public places whose content is pornographic, racist, discriminatory, insulting or offensive, or sending messages containing such content;
- sending messages with content whose nature is that of sexual or other harassment or any message that incites or may incite discrimination, hatred and/or violence;
- sending messages to large numbers of recipients simultaneously, transmitting chain letters or disseminating malicious software, such as viruses, ransomware or spyware;
- disseminating fake news or disinformation;
- using file-sharing or streaming services that generate excessive data traffic to the extent that this may affect the availability of the Facilities;
- downloading films, music, software or other copyright-protected material from any illegal source or if you know or ought to know that this infringes copyright;
- distributing (uploading) films, music, software or other copyright-protected material to other parties without the consent of the rightsholders.

The Facilities may only be used for students' own commercial activities if WU consents to this in writing in advance.

The use of our network facilities in a student residence on campus is unlimited except insofar as it is required to ensure the integrity and security of the network or to limit the consequences of congestion. If we intervene to limit the consequences of congestion, identical types of traffic will be treated in the same way. The other provisions of these regulations will apply in full when you use our network facilities at home.

1.3. Intellectual property and confidential information

As a student, you are expected not to infringe our intellectual property rights or those of any other party and to respect any licensing arrangements that apply within WU.

Control over any WU information, such as that applicable pursuant to educational examination records and where the confidentiality of examination questions is involved, for example, is vested in us. As a student, you do not control such information in your own right except where WU explicitly assigns it to you.

Unless required for your studies, you may not download large numbers of articles from or systematically copy substantial parts of the files or databases in the electronic library.

If you receive access to confidential or privacy-sensitive information from us for the purposes of your study, you are required to treat it in strict confidence.

In this case, we expect you to devote special attention to the adoption of the measures mentioned in Article 1.1 (Security) of these regulations. This applies in particular to the performance of tasks that require confidential information to be processed beyond WU's control, such as email or its inclusion in cloud applications not linked to the organisation or students' own equipment or storage media. For the security purposes, you are always required to use the applications that WU offers where possible.

You are required to comply with the applicable legislation and regulations when processing confidential or privacy-sensitive information. In the event that we draw up additional rules to safeguard confidentiality and intellectual property rights, you will also be required to ensure strict compliance with them.

2. Oversight and monitoring

We monitor compliance with these regulations. When monitoring the use of the Facilities, we will act in accordance with the applicable legislation and regulations.

For the purposes of such oversight and monitoring, we will seek to adopt measures that confine access to privacy-sensitive information or personal data of individual students as far as possible. In this respect, we will act on the basis of pursuing an appropriate balance between oversight and monitoring for the purposes of enforcing these regulations and protecting your privacy. Where possible, we will pursue automated oversight or filtration without gaining an insight into the behaviour of individuals.

2.1. Conditions governing oversight

The use of the Facilities will only be overseen and monitored for the purposes of enforcing the rules set out in these regulations and solely for the purposes mentioned in Article 1. It is important that this occurs to uphold the good order and to safeguard the integrity and security of our Facilities.

2.1.1. Monitoring incidents

Monitoring and logging

In order to oversee any threats to the integrity, availability and confidentiality of WUR systems, all activities and information of all users of the Facilities will be constantly processed automatically (monitoring and logging).

Such logging data will be processed using automated procedures that may result in an alert being raised in accordance with predetermined rules.

Analysis of incidents

Only if it follows from the predefined rules that a system alert constitutes grounds for further investigation (for example, the detection of a virus or irregular login attempts) will the administrators of the relevant service and/or external or other analysts conduct further analysis of such alerts. Part of such an analysis may involve tracing an alert to a system or individual. This means that at that point in time a WUR system administrator or external analyst may gain access to the nature of the

information and activities of the relevant WUR student insofar as the alert concerns them (e.g. the content of a phishing message).

In an emergency or where required to ensure that a risk of harm does not materialise (or do so further), these staff members may decide to adopt technical measures, such as blocking access to a particular service or limiting the capabilities of the equipment in question to enable the network to be used. This will always involve temporary measures for no longer than the duration of the incident. Where the situation allows this, the information security officer (ISO) will assess whether the measure is appropriate in advance. In an emergency the ISO will be notified as soon as possible after the measure has been adopted.

2.1.2 Monitoring an individual

Where WU suspects that a student has contravened the rules, focused monitoring may occur for a fixed (brief) period, and this may be logged as provided for in Article 2.1.1. Such monitoring will only focus on content should it appear that there are compelling reasons for doing so. The procedure for a targeted investigation is set out in Article 2.3.

2.2. Conducting general oversight

In order to oversee compliance with these regulations, we may adopt several specific measures, namely:

- We may monitor leaks of confidential information to which you have access for the purposes of your studies or to perform assignments for us with the aid of random content filtering. In this respect, suspect messages may be set aside for closer examination.
- We will also conduct checks for the purposes of cost and capacity management limit to examining the sources of costs or capacity demand based on traffic data. Where such sources result in major expenditure or inconvenience, they will be blocked or limited without infringing confidentiality with regard to the content of the relevant communications.

2.2.1. Attack simulations and social engineering

In order to identify vulnerabilities, it is necessary to conduct attack simulations and carry out social engineering on the Facilities. Such attack simulations and social engineering are only conducted in consultation with the ISO and with its formal consent. In the case of social engineering, privacy risks are identified beforehand and mitigated as far as possible in consultation with the data protection officer (DPO) and with the help of a data protection impact assessment (also known as a DPIA).

Red teaming and pen tests are examples of such activities. Operations for the purposes of attack simulations and social engineering are carried out in line with the applicable privacy legislation. For example, personal data may be collected in the following ways in the case of attack simulations and social engineering:

- Social engineering: a user may be enticed to perform certain action or to surrender information, such as their password.
- Attack simulation: An attempt may be made to log into a device or system (for example, the student information system) using an account with more privileges, thereby making it possible to view folders and files potentially containing personal data and other information of a confidential nature.

Arrangements are made with the testing party to ensure that any personal data found is dealt with in confidence. Any personal or other data that is found will not be

stored for longer than is necessary for the purposes of the test. Personal and other data will be secured appropriately. Any folders or files that are explicitly designated as 'personal' will not be examined unless it is reasonably impossible to avoid this.

2.3. THE PERFORMANCE OF TARGETED INVESTIGATIONS

A targeted investigation occurs when traffic data or other information concerning a specific student is recorded and analysed to check whether any actual breach has occurred based on concrete indications of any breach of these regulations.

We may conduct a targeted investigation based on a compelling suspicion that a student has contravened these regulations. We will only conduct a targeted investigation after the Facilities and Services Director issues written instructions to this effect and after obtaining advice from the CISO and the DPO, who will cite reasons as to why such instructions have been issued. The Executive Board will receive a copy of the instructions and an aggregated summary of the findings of the investigation. In the event that the advice provided by the CISO and/or the DPO differs from the instructions issued by the Facilities and Services director, the Executive Board will need to consent to the instructions to conduct an investigation in advance. Where an investigation does not yield any grounds for additional measures, anything that has been recorded will be anonymised or destroyed.

Based on the concrete indications mentioned in Article 2.1.1, we may also conduct a targeted examination of the security or integrity of automated systems or peripheral equipment (such as routers or printers). In derogation from what is stated above, written instructions from the Facilities and Services Director will not be required in this case. The findings of this examination will only be shared for the purposes of improving the security and integrity of the peripheral equipment.

A targeted investigation based on a compelling suspicion of a breach of these regulations will, in the first instance, be confined to data obtained from logs that are already available, such as those of an individual user or system, as mentioned in Article 2.1.1. Should a targeted investigation yield additional evidence, we may proceed to familiarise ourselves with the content of the relevant communications or saved files. This will again require the written consent of the Facilities and Services Director, in accordance with the procedure set out above, who will cite the reasons as to why consent has been granted.

The following are several specific personal measures that we may adopt for the purposes of oversight:

- Monitoring the leakage of confidential information. This will occur on the basis of random tests based on keywords. Suspicious messages will be retained for closer investigation in consultation with the Executive Board.
- Checking for the prohibited use of email and other electronic means of communication. Two individuals will do this by opening electronic messages and consulting their contents based on a convincingly substantiated complaint. These individuals will be bound by a duty of non-disclosure in relation to the content.

If you are suspected of having contravened these regulations, the Facilities and Services director will notify you of the grounds for, the conduct of and the findings of the investigation within three weeks. You will be afforded an opportunity to explain your position concerning any information found. This notice may only be delayed if it

could harm the investigation and only for the period that is necessary to take any disciplinary action. Advice will be obtained from the DPO beforehand.

Except in urgent circumstances or where there is a clear suspicion that these regulations have been breached, WU staff members who are directly responsible for overseeing and monitoring compliance with these regulations only have access to the content of the relevant documents, email messages or other files if you consent in writing. In that case, you will be notified of the findings of the investigation afterwards.

2.4. Ensuring privacy during monitoring

We process the personal data of the Facilities users, the content of communications or saved files when overseeing and checking compliance with these regulations and monitoring the Facilities. When overseeing and monitoring at the level of personal data, we comply in full with the GDPR and other relevant legislation and regulations referred to in this article.

2.4.1. Measures for the purposes of privacy

Purpose limitation
We process students' personal data solely for the purpose set out in Article 1.

Accuracy
For the purposes of monitoring in relation to these regulations, we adopt the requisite measures to ensure that personal data is appropriate and accurate given the purpose for which it is processed.

Data minimisation
We have structured the monitoring procedure in such a way that the processing of personal data remains confined to what is required for the purposes referred to in Article 1 by, amongst other things, ensuring that the use of the Facilities will only be monitored through automated processing in the absence of any automated decision-making. Administrators and external or other analysists may only gain access to the content of students' internet, data and email traffic in the case of a concrete alert or a targeted investigation.

Storage limitations
Any personal data recorded for the purposes of overseeing and monitoring compliance with these regulations will be stored as briefly as possible. Only when there is a reasonable suspicion of unlawful use, may this period be extended for as long as is required to complete the investigation to be conducted in response. Once an investigation has been completed without leading to disciplinary measures against the person involved, the relevant information may be anonymised or deleted. Where an investigation does lead to disciplinary measures, the relevant information will be retained as long as necessary for evidential purposes or for the enforcement of disciplinary measures.

Integrity and confidentiality
We will also adopt appropriate technical and organisational measures to secure any personal data recorded for the purposes of overseeing and monitoring compliance with these regulations against their loss and/or any form of unlawful processing. This may include the following measures, amongst others:

- with the aid of technical, organisational and legal measures, we will ensure that WUR staff and external parties cannot gain access to the content of personal or other data except insofar as is stipulated in these regulations;
- only those staff will have access to personal data where such access is required for the purposes of performing their work;
- furthermore, all staff who are required to familiarise themselves with personal information for the purposes of oversight and monitoring in relation to these regulations will be contractually bound to observe an additional duty of non-disclosure, except where any provision of the law renders such disclosure mandatory or the need for it follows from their duties;
- WUR will periodically assess whether the administrators of the service comply with the arrangements that apply in relation to them with regard to authorisation, purpose limitation and non-disclosure when carrying out their work.
- We will periodically assess whether those parties with whom such data is shared comply with the arrangements that have been made.

2.4.2. Other parties

We only share recorded personal data with another party if it is necessary to do so for the purposes of conducting an investigation and enforcing disciplinary measures. As such, we may pass on personal data to the police where a criminal offence is suspected or found to have been committed. Where WUR shares personal data with an external organisation, we will ensure that binding arrangements are made concerning the its processing by an external party, and that satisfy the principles stipulated in Article 28 of the GDPR at least.

Supplying personal email correspondence or information on data carriers belonging to WU or granting access to the email correspondence and information of a deceased person to their surviving relative(s) in some other way cannot be reconciled with the deceased's integrity interest and the relevant correspondence partners' privacy interests[1]. It will only be possible to transfer any information that is requested – subject to certain guarantees – to a reliable, independent agency selected in consultation with WU, which will assess that information and then request consent for its release from those interlocutors. The applicant is required to engage this agency itself and to bear the costs involved.

2.4.3. Data subjects' rights, contact details and general provisions

The WUR Personal Data Protection Regulations govern personal data processing for the purposes of these regulations. Click here for more information on how WU deals with personal data, such as the options for exercising rights under the terms of the GDPR.

3. Implications of breaching these regulations

In the event of a failure to comply with these regulations or the applicable legislation and regulations and standards of decency when using the Facilities, depending on its nature and gravity the Executive Board may take disciplinary action, block the Facilities or institute legal proceedings.

[1] After all, it is important to respect the fact that no more may be revealed concerning such email correspondence than what the deceased and their correspondence partners themselves would have wished to reveal.

3.1 Disciplinary action

This includes warnings, reprimands, the temporary reduction or closure of the Facilities (for no more than a year) and, in extreme cases, the termination of registration as a student.

We may not take disciplinary action (except for a warning) merely on the basis of the automatic processing of personal data, such as detection with the aid of an automatic filter or block. In addition, no disciplinary action may be taken without you being afforded an opportunity to explain your position.

Insofar as no other appeal procedure is available, you are entitled to object against our decision to proceed with disciplinary action. You may approach the Student Legal Protection Desk at legalprotection.students@wur.nl for this purpose. An objection must be lodged in writing within six weeks after the date of the relevant decision. If you disagree with the outcome of objection proceedings, you may lodge an appeal in writing with the Higher Education Appeals Tribunal within six weeks of the date of the ruling on the relevant statement of objection.

3.2 Blocking access to Facilities

Should a breach or suspicious behaviour be detected, we may block access to the relevant Facilities temporarily by automatic or manual means. Such a block will be maintained until it is shown that the cause has been eliminated. Should the cause be repeated, disciplinary action may be taken.

3.3 Pressing charges and compensation

Following documented consultation with the most appropriate disciplines within WU, we may press charges at any time in the case of a suspected or detected criminal offence. Where our assistance is requested in the case of a criminal investigation, we will provide assistance in accordance with the law. Acting at the Executive Board's behest, WU may recover any losses suffered as a result of a contravention of these regulations.

4. Final provisions

The Executive Board may amend these regulations. Amendments will only be introduced at the start of an academic year, except in pressing circumstances or if external circumstances compel us to do so sooner.

An amendment will only be introduced after the participational structure of the relevant organisation has consented to it. The Executive Board will consider student feedback before introducing an amendment.

In any situation that is not covered by these regulations, a decision taken by the Executive Board will be final.

These regulations were adopted on March 29, 2022 and will be effective from September 1, 2022.