Network Regulations Wageningen University & Research

(regulations for using the IT-facilities)

20160905 Network Regulations Wageningen University en Research
update of version 2016010 regarding change of name Wageningen University & Research

Table of Contents

Basis for the Network Regulations

Wageningen University and Research Centre[1] (WUR) provides Internet and IT resources to students, employees and other users at WUR. These facilities are necessary for employees to do their jobs properly or for students to study effectively. However, there are risks involved that necessitate the establishment of clear rules of conduct. Within the context of these risks, all users must be held accountable to use WUR's provided Internet and IT resources responsibly.

With these Network Regulations, WUR wishes to establish rules regarding the desired use of WUR's Internet connections (including e-mail facilities) and all IT resources. The goal is to provide a good balance between responsible and secure IT and Internet use and user privacy.

The use of social media (including Facebook, LinkedIn and Twitter) is indispensable these days, but can also have negative repercussions for WUR. For this reason, WUR also wishes to set down certain rules for social media use.

In legal terms, WUR is not only an employer, but also a network administrator and, as an employer, is authorised to establish rules concerning how work is performed in order to create an efficient workplace. As an institute for higher education, WUR has the legal right and responsibility to set down rules regarding proper procedures to be observed in the institute's buildings and premises (Article 7.57h of the Higher Education and Research Act (WHW)). In addition to this Act, these Network Regulations are also based on articles from the Collective Labour Agreement Dutch Universities (CAO NU) and the Collective Labour Agreement Stichting Wageningen Research (CAO Stichting Wageningen Research).

Given that the Network Regulations include the processing of personal information and/or monitoring the behaviour and performance of employees and students, it must be approved by Wageningen University's Central Works Council and Student Council.

The Network Regulations are in line with other regulations, such as WUR's Data Protection Regulations and Information Security Policy as well as the terms of use for SURFnet and WUR's connectivity provider.

[1] Wageningen University & Research is a partnership between the public legal entity: Wageningen University and the private legal entity: the foundation Stichting Wageningen Research

1 Basic Principles

1.1 The Network Regulations set out rules regarding the use of WUR's IT resources and Internet connection. The goal of these regulations is to produce clear guidelines with respect to:

- the system and network security, including safeguarding against harm and abuse;
- prevention of sexual harassment, discrimination and other prohibited acts;
- protection of WUR's confidential information, including processed personal information of employees and students, parents and third parties;
- protection of WUR's intellectual property rights and those of third parties (e.g. licensing agreements and research data);
- prevention of deliberate and repeated unjustified actions that could harm WUR's good reputation with reference to article 6, Social Media Use;
- cost and capacity management.

1.2 Limited private use of WUR's Internet and IT resources is permitted provided that it is not disruptive to others, to daily work activities or to the proper functioning of WUR's network. Its use for ancillary activities (nevenwerkzaamheden) or commercial purposes is forbidden at all times unless special prior written permission has been obtained.

1.3 These Network Regulations apply for every user of WUR's Internet and IT facilities.

1.4 A user is defined as: any person who makes use of the IT or Internet facilities (wired or wireless) that WUR has made available, whether through an ICT workstation or a computer, laptop/notebook, smartphone, etc., including via remote access. These users include students, employees, staff hired by WUR, external parties (including relations) and guests;

1.5 A student is defined as: any person who is enrolled as a student or follows a programme at WUR.

1.6 An employee is defined as: any person referred to in the Collective Labour Agreement for Dutch Universities and the Collective Labour Agreement STICHTING WAGENINGEN RESEARCH and anyone employed by Wageningen University and the STICHTING WAGENINGEN RESEARCH Foundation.

1.7 These Network Regulations also apply in cases in which other institutes provide guest access to their network facilities based on the login information of one's own institute (Eduroam).

1.8 WUR must take all reasonable measures to protect sensitive data, including limiting access to sensitive information or personal information of individual users as much as possible. This involves automated monitoring or filtering where possible, without WUR or any third parties having access to observe the behaviour of individual persons. All reasonable measures will be taken to immediately delete or correct any personal information that is inaccurate or that deviates from the purposes for which it was processed.

1.9 The Director of Facilities & Services of WUR has been appointed as Supervising Authority by the Executive Board and, thus, is responsible for the management of IT facilities and for monitoring the above basic principles.

2 Intellectual property and confidential information

2.1 Users will not infringe the intellectual properties of WUR or any third parties and will respect the license agreements that apply to WUR.

2.2 WUR remains responsible for all information from WUR. Users have no independent control over information except to the extent to which they are entitled to this by law and/or the CAO, unless deviations have been agreed to or express written permission has been given by WUR.

2.3 Users shall handle all confidential and/or sensitive information, including personal information to which they are privy in the course of their work or study, in strict confidence and take all necessary measures to ensure the confidentiality thereof.

2.4 Users shall pay particular attention to ensure they adhere to the measures stated here in these Network Regulations if the processing and/or storage of confidential information outside WUR is necessary in the performance of work-related activities or in order to follow a study programme. This includes information that is shared or stored via e-mail, in third-party cloud applications, on external storage devices and personal devices (e.g. USB devices, tablets, and smartphones). WUR has established confidentiality regulations[2] with respect to information security and ensuring confidentiality.

2.5 Users are not permitted to download large volumes of content from the files in the digital library or systematically download or copy substantial portions of files or databases in the digital library. Downloading is in principle permitted if it is work and/or study related.

2.6 These provisions apply in particular to IT managers and functional administrators who breach these regulations. This is considered a serious dereliction of duty in view of their particular position.

[2] https://www.intranet.wur.nl/en/services/ict/informationsecurity/Pages/WUR-information-security.aspx

3 Use of IT equipment and network facilities

3.1 IT equipment and network facilities are provided to users for the performance of their duties or studies through strictly confidential personal login information. Private use of these resources is only permitted if in accordance with Article 1.2. Disruption of WUR's wireless networks through radio activity should be avoided. Users are required to contribute to solutions to prevent this.

3.2 Users must at all times treat the personal login details assigned to him/her and any additional authentication methods (such as smart cards and tokens) with the utmost care. Users may provide authorisation to a third party to access their e-mail facility, including their calendars. However, the third party must use his/her own login information for this. Personal passwords and additional authentication methods may not be shared or used for access to other non-WUR systems. In case of suspected password abuse, the IT manager can directly block the account in question.

3.3 Connecting servers, local storage facilities (such as NAS) and active network components (such as access points and routers) is only permitted with the approval of IT management and only if the stability and/or integrity of WUR's systems are not overloaded. In order to have approval granted, IT management may stipulate rules in order to uphold these Network Regulations, including requirements to install virus scanners and password protection. WUR may forbid the use of specific software if it deems it necessary (in terms of security or if the software cannot be modified for all security risks). It is always forbidden to install and use software in the performance of tasks for WUR which is only licensed for private use.

3.4 Connecting personal mobile devices (such as laptops, tablets and phones) is only permitted on the network connections made available for this purpose. IT management may stipulate rules for the access of these facilities in accordance with the connection conditions[3]. This may include specific settings, password security, compulsory use of a virus scanner or an encryption program. The owners of personal devices are responsible for up-to-date protection on their devices and are personally accountable for any actions which were carried out from their personal equipment.

3.5 Data from private mobile devices which is synchronised in any way with WUR's systems, including all information and messages that are created, saved, sent or received and are incorporated into the synchronisation procedure, is considered to be WUR data. As such, this data is subject to the same control measures as all other data and devices from WUR.

3.6 Loss or theft of any equipment that contains data from WUR or any mobile device which automatically synchronises with WUR's network, must always be reported immediately to IT management (IT Service Desk), regardless of whether the equipment is private or owned by WUR. Failure to report such a loss or theft will lead to the consequences for violations mentioned in article 10. The IT management will then halt the synchronisation and (if possible and necessary) erase the data on the device. WUR is legally obliged to report all data breaches immediately to the Dutch data protection authority.

3.7 Before damaged or defective personal equipment with WUR data on it may be released for repair or disposal within WUR or elsewhere, all existing data on the device must be erased as thoroughly as possible.

3.8 The storage of private data on WUR systems is permitted, provided that it is properly marked as such through clearly naming the relevant files and folders and provided this does not overload the capacity of these systems or disrupt the good functioning within the workplace. However, WUR is not obliged

[3] https://www.intranet.wur.nl/en/services/ict/klantenservice/beleid_afspraken/Pages/WUR-beleid-en-afspraken.aspx

to make backups of such files or information, or provide copies when replacing or repairing the relevant systems and it is not liable for the loss or damage of such information.

4 Use of e-mail and other IT communication resources

4.1 The e-mail system and the corresponding mailbox and e-mail address are provided to users within the context of their jobs, studies or specific relation with WUR. Use of these is thus directly related to the tasks arising from the job, study or specific relation with WUR.

4.2 Private use these resources is only permitted as specified in Article 1.2.

4.3 However, using IT communication resources (whether private or work related) for the following is forbidden at all times:

- *sending messages with pornographic, racist, discriminatory, threatening, insulting or offensive content;*
- *sending messages involving sexual harassment or other undesirable behaviour as described in the Wageningen University & Research Integrity Code[4];*
- *sending messages that could result in incitement to discrimination, hatred and/or violence;*
- *sending unsolicited messages to large numbers of recipients, passing on chain mail or disseminating malicious software such as viruses, trojans or spyware.*

4.3 Users must not use their WUR e-mail address for private mail. WUR will not block access to other e-mail services for private use, nor will it specifically monitor them.

4.4 In case of illness/disability, death, long-term absence, poor performance or gross negligence by users (but only if such puts company interests at serious risk), WUR is authorised to grant access to the content of the user's mailbox by a manager or substitute. However, access will only be granted if it can be proven that the authorisation cannot be acquired from the user within a reasonable amount of time or if the management council of the organisational unit or the Executive Board[5] deems that the company's interests are too greatly at risk that consent is not required or that the situation is too urgent to wait (pressing interest). In the latter case, such a request for access must be submitted to the Executive Board by the Supervising Authority.

4.5 In addition to the provisions in the preceding Article, the manager/substitute may not access any folders marked as private, correspondence identifiable as private, or e-mails sent to or received from a confidential counsellor, in-house medical officer or HR consultant. If the user has not clearly identified what is private in accordance with Article 4.5, WUR will call in a confidential counsellor who will check the relevant information of the employee in order to identify private information and demarcate it so that the substitute or manager does not become privy to such private information.

4.6 E-mail messages and files from members of the participational body, in-house medical officers, HR consultants and anyone whose occupations are granted confidentiality under the law, will never be checked. This does not apply to automated control of the security of e-mail and network traffic.

[4] http://www.wur.nl/en/About-Wageningen/Corporate-governance.htm

[5] Executive Board of WUR: Board of Governors Wageningen University and/or Board of Governors Stichting Wageningen Research

5 Internet use

5.1 Access to the Internet and related facilities are made available to users within the context of their jobs, studies or specific relation with WUR. Use is thus related to the tasks arising from the job, study or specific relation with WUR.

5.2 Private use of these resources is only permitted in accordance with Article 1.2. Use of the WURnet account, whether private or study-related, must not be disruptive to the good functioning of WUR, must not cause nuisance to others, must not infringe on WUR's rights or those of third parties and must not threaten the integrity and security of the network.

5.3 The following activities fall under the category of 'disruptive and/or causing nuisance':

- using or setting up Internet services in public areas with pornographic, racist, discriminatory, offensive or objectionable content, or sending messages with such content;
- sending messages involving harassment, sexual or otherwise, or messages that could provoke incitement to discrimination, hatred and/or violence;
- sending messages to large numbers of recipients, passing on chain mail, the 'mining' of bitcoins or disseminating malicious software such as viruses, worms, trojans and spyware;
- using file sharing or streaming services if they generate excessive traffic and therefore potentially jeopardise the availability of the facilities or if it interferes with others' work;
- downloading films, music, software and other copyright protected material from any illegal source or if the user should have known that this is in breach of copyright;
- disseminating or uploading films, music, software and other copyright protected material to third parties without consent of the copyright holders;
- disseminating or otherwise communicating WUR's confidential information and intellectual property to third parties without WUR's permission.

5.4 Users who use WUR's computer and network facilities outside WUR buildings via a WUR account with the automated login, must adhere to these Network Regulations. Users who are not logged in with the WUR account but still use WUR's network facilities through a private account, must still adhere to these Network Regulations. Other than this, no other restrictions apply for private Internet use outside WUR's buildings. In such cases, only Dutch law is applicable for private use.

6 Social media use

6.1 WUR supports open dialogue and the exchange of ideas and the sharing of knowledge with colleagues and third parties via social media (e.g. Facebook, YouTube, Instagram, Skype, Twitter, Yammer or LinkedIn).

6.2 Executives, managers, and others who convey knowledge, policy or strategy on behalf of WUR, have a special responsibility when using social media, even if the content is not directly connected to their work. By virtue of their position, they must determine whether publishing certain things in a personal capacity is the best idea. They must be aware that employees and others are sure to read what they write. WUR has specific guidelines regarding the style of presentation and communication[6].

6.3 These Regulations also apply when social media is used from private computers or Internet connections, but only insofar as it is work related (or concerns WUR).

6.4 If a social media account is set up that is work related or involves WUR, but is set up as a personal account in the name of an employee, the employee and WUR should find an amicable solution for transferring this profile or the information and contacts thereon if the employment relationship is terminated.

[6] See http://www.wageningenur.nl/nl/Over-Wageningen-UR/goto/Social-Media.htm

7 Monitoring and control

7.1 Monitoring the use of IT facilities and the Internet occurs solely within the context of the enforcement of the rules of the Network Regulations for the purposes stated in Article 1 and to ensure that Internet usage functions properly. In cases where these regulations are violated, the involved user will be approached by the supervisor regarding his/her responsibilities, while technical measures against prohibited use will be taken wherever possible to limit or deny access.

7.2 For the purpose of monitoring compliance with the rules, data is collected and logged through an automated process. This information is only accessible to the IT management directly responsible and provided to the Supervising Authority in anonymised form whenever possible. Based on this information, further technical measures may be taken.

7.3 In the event of suspected violation of the rules, an IT and Internet check can be conducted at the individual traffic data level. The checking of content will only occur if the violation is particularly serious.

7.4 At all times, WUR abides by the Data Protection Act and other relevant laws and regulations when conducting such checks at the traffic data or personal information level. WUR takes particular care to secure the data obtained in such checks from unauthorised access and all individuals with access to it are contractually obliged to maintain confidentiality.

7.5 Some specific control measures that WUR can take are:

- monitoring within the context of system and network security (including malware and spam) based on the filtering of content using keywords;
- monitoring within the context of cost and capacity management is limited to checking based on traffic data from the sources of costs or capacity demand (such as addresses of Internet radio and streaming sites). If these websites result in great expense or inconvenience, they will be blocked or restricted, without violating the confidentiality of the contents of the communication;
- monitoring of the use of images is based on complaints or reports or through the random sampling of images that are publicly available.

7.6 Within the context of the Help Desk, IT management will only provide access to users' accounts or WUR-provided devices if a user has given his/her consent for this. Access without such consent is only permitted in urgent cases or upon warranted suspicion of violations of these Network Regulations as specified in this Article. If reasonably possible, users will be informed after such access has taken place.

8 Procedure for targeted investigation

8.1 Targeted investigations have the following aims:

- determining whether improper IT and/or Internet use has taken place;
- monitoring agreements;
- verifying that confidential information is adequately protected and is not disclosed or will not be disclosed;
- preventing deliberate and repeated unjustified negative publicity about WUR by means of using the WUR Network;
- compliance with legal obligations to provide data from the investigation to third parties.

8.2 Targeted investigation occurs when a user's traffic data or personal information is logged within the context of an investigation, following warranted suspicion of violations of the Network Regulations by a user.

8.3 Targeted investigations on traffic data only occurs following a written mandate by the Supervising Authority and approval from the Executive Board. If deemed appropriate, a copy of the investigation's results will be submitted to the Executive Board. The manager will always receive a copy of the results. These results will be handled in a strictly confidential manner.

8.4 If users contravene these regulations, these users will be called to account for their behaviour as soon as possible by the manager or Supervising Authority. These users will be asked to give an account of the data discovered. Postponing this information may only occur if the investigation could be harmed by disclosing this information.

8.5 Targeted investigation is initially limited to the traffic data and personal information of the use of the IT facilities. WUR will exercise restraint in collecting this data.

8.6 If a targeted investigation yields further evidence, the content of communications or saved files may also be examined. A targeted investigation will then be conducted into the offending user. WUR will make every effort keep the identity of the people who conduct the examination of the users' communication and/or files strictly confidential.

9 User rights regarding personal information

9.1 Users can request the Executive Board for a complete overview of all their personal information that is processed by WUR in the context of the Network Regulations. Such a request will be met within four weeks.

9.2 Users may request the Executive Board to update, add to, delete or block their personal information if it is factually incorrect, incomplete or irrelevant for the purpose or is contrary to a statutory regulation. Such a request will be processed within four weeks. If the request is refused, reasons will be provided. An approved request will be carried out as soon as possible.

9.2 Additionally, users may formally object to the processing of their personal information in connection with grave personal circumstances. The Executive Board will decide whether the objection is justified within four weeks after receipt. If the Executive Board deems the objection to be justified, processing will be terminated immediately.

10 Consequences for violations

10.1 In case of non-compliance with these Regulations or the general applicable statutory provisions, the Executive Board may, depending on the nature and severity of the offense, take disciplinary measures. For violations by students, disciplinary measures can be taken on the basis of Article 7.57h of the Higher Education and Research Act (WHW). Students may appeal the decision to the Appeals Tribunal for Higher Education (CBHO). In cases of violations by employees of Wageningen University or the Stichting Wageningen Research, disciplinary measures may also be taken as stated in the regulations on the WUR intranet site. Violations committed by users who are not covered by the CAO NU and the CAO Stichting Wageningen Research, but are accountable to the Executive Boards, may result in the termination of the employment relationship with WUR. For users such as external parties and guests, appropriate measures will be sought. In all cases, proportionality between action(s) and appropriate measures will be taken into account.

10.2 Disciplinary measures (other than a warning) may not be taken based solely on automated processing of personal information, for instance when an automatic filter or blocker is detected. Furthermore, no disciplinary action will be taken without providing users the opportunity to present their side.

10.3 In deviation from/supplementary to the preceding articles, the Executive Board may temporarily block the relevant facility if a disturbance is detected through automated monitoring processes. This block will be maintained until it is demonstrated that the cause has been removed. Disciplinary action may result in cases of repeated disturbance.

10.4 In the event of serious security incidents and emergencies, IT management is authorised to restrict facilities or shut down portions of the network entirely. WUR will report any evidence of criminal acts to the police.

10.5 WUR reserves the right to claim for possible damages caused by improper use of the facilities or non-compliance with the Network Regulations by users, in accordance with private law.

11 Final provisions

11.1 These Network Regulations are evaluated once every three years by the Executive Board together with the Participational Body.

11.2 With the consent of the participational body, WUR may change these Network Regulations as the circumstances warrant. Changes will only be introduced after the Student Council has been consulted. Planned changes will be announced to the employees/Central Works Council (COR) and the students/Student Council prior to their introduction. The Executive Board will consider feedback from students and staff before making any changes. WUR's participational structure approved the content of these Network Regulations on December the 11th, 2015. These Network Regulations will be effective as from January the 1st, 2016.

11.3 In cases not covered by these Network Regulations, the Executive Board will make a final decision.

11.4 These Network Regulations will be published on WUR's Internet/intranet site.