

WUR Regulations for Network

Privacy Regulations for Network Use at Wageningen UR

Containing a description of the use of personal information related to the use of the network by individuals to whom Wageningen University and Research Centre provides network access.

These regulations have been compiled with attention to the Personal Data Protection Act (WBP; Stb. 2000, no. 302); they have been approved by the Executive Board, the Central Employees Council and the Student Council.

RESOLUTION:

Section 1 Definitions

As used in these regulations, the following terms are defined as shown.

- **WUR:** Wageningen University and Research Centre, the framework of cooperation between Wageningen University and the DLO Foundation, also called Wageningen UR;
- **Executive Board:** the Executive Board of Wageningen University and DLO Foundation;
- **WURnet:** the computer network of Wageningen UR;
- **Internet:** the external network to which the WURnet is linked;
- **Organisational unit:** a part of the organisation (for example, department, institute or office), or a legal entity related to Wageningen UR, which makes use of WURnet via the technical infrastructure made available by Wageningen UR;
- **Competent authority:** the head of an organisational unit. With respect to the head of an organisational unit of Wageningen UR or a student, this is the Executive Board of Wageningen UR;
- **HRM:** the Human Resource Management office of Wageningen UR;
- **FB:** the Facilities Service of Wageningen UR;
- **FB-ICT:** the ICT division of the Facilities Service;
- **System administrator:** the individual at the FB-ICT who administrates the infrastructure that provides access to WURnet and the Internet;
- **Code of behaviour:** the code of behaviour for using the computer facilities of WUR, especially e-mail, WURnet and the Internet;
- **User:** the individual to whom Wageningen UR provides access to WURnet and thereby to the Internet;
- **Student:** an individual who is enrolled at an educational institute of Wageningen UR;
- **Employee:** an individual who has a employment relation with, or conducts activities for, Wageningen UR;
- **User name:** the name assigned to a user for computer use;
- **Network use:** any use of the access offered by Wageningen UR to WURnet and the Internet, emphatically including the use of e-mail and the World Wide Web;
- **IP address:** Internet Protocol address; a unique access number to WURnet and the Internet that is linked to the workplace of the user;
- **Logging:** the automated storage of data in a file concerning the actual use of the network, including both WURnet and the Internet;
- **Monitoring:** the focused monitoring of the use and the functioning of the network, by using the data acquired from logging and other information.

Section 2 Applicability

These regulations apply to monitoring and processing information concerning the network use of a user.

Section 3 Aim

The aim of the processing referred to in Section 2 is to be able to monitor compliance with the code of behaviour for the use of network facilities that are covered by this privacy regulation.

Section 4 Logging

Every use of access to the network can be recorded by means of logging.

Section 5 Monitoring

- 1) If there are ready indications of network use that is in conflict with the code of behaviour, monitoring can be used as referred to in Section 2.
- 2) Monitoring as referred to in 5.1 will not be applied except following an order provided by the Executive Board to the Director of the Facilities Service (FB), this decision being the result of a written request made by the competent authority of the relevant user. If an employee is involved, the intervention of the Director of HRM is required.
- 3) Monitoring as referred to in 5.1 can also be applied following an order from the Executive Board in the cases referred to in Section 43 of the Personal Data Protection Act.
- 4) A decision to implement monitoring will be disclosed only to the individual making the request, the relevant competent authority, the Director of the Facilities Service, the head of the FB-ICT and the system administrator who is responsible for the monitoring.
- 5) The individual being monitored will be informed of the decision to implement monitoring within 24 hours.
- 6) Monitoring is implemented by the system administrator.
- 7) Monitoring will not be implemented for a longer period than is strictly necessary.

Section 6 Target group

The information to be processed concerning network use contains only data about users and their use of WURnet and the Internet.

Section 7 Information to be processed

- 1) Subject to the situation referred to in 7.3, logging of network use within the scope of these regulations will provide only the following information:
 - a. information about access to the Internet which is offered by Wageningen UR to the user, including the user name and the IP address;
 - b. information concerning the date and time of opening and closing the access to WURnet and the Internet by the user.
- 2) FB-ICT has access to more information concerning network use, including the IP addresses of the links with internet sites.
- 3) If the Director of the Facilities Service has received an order to conduct monitoring as referred to in Section 5, Subsection 2, then the information as referred to in 7.1 is linked to the data referred to in 7.2 via the IP address.
- 4) From the moment this linkage is in place, monitoring as referred to in Section 2 provides information concerning the Internet sites visited by the user and the time when the user visited certain Internet sites.

Section 8 Direct access to information

Direct access to the information referred to in Section 2 is possible only for:

- a) the system administrator and individuals commissioned by the head of the FB-ICT who are mandated to collect, link and delete information on behalf of the Director of the Facilities Service;

- b) individuals who, pursuant to statutory provisions, are authorised to have access due to the intervention of the Executive Board.

Access is provided only after signing a declaration of confidentiality.

Section 9 Preconditions for providing information

Information as referred to in Section 7 can be provided by the Director of the Facilities Service to the competent authority only if there are clear indications of network use by the relevant user that are in conflict with the code of behaviour.

Section 10 Provision of information

Information as referred to in Section 7 can be provided outside the organisational unit of the relevant user only to the following:

- a) the Director of HRM (only if the relevant user is an employee);
- b) the head of the FB-ICT section, who, on behalf of the Director of the Facilities Service, is mandated with or provides leadership to the investigation into network use that is in conflict with the code of behaviour;
- c) the system administrator as referred to in Section 1;
- d) the Executive Board;
- e) the judicial authorities or a judicial organisation.

Section 11 Retention period

- 1) The information obtained from logging will be retained and made available for the objective as formulated in Section 3 for no more than one month.
- 2) Information obtained from logging that is older than one month will be discarded, unless the competent authority believes there are indications of network use that is in conflict with the code of behaviour during that month and a request has been made to the Executive Board as referred to in Section 5, Subsection 2.
- 3) If a system administrator is unable for technical reasons to remove information obtained by logging or monitoring within three months, discarding will be defined as no longer making this information available for the objective as formulated in Article 3.
- 4) In a case such as that referred to in 11.2, the information obtained from logging will be retained for a longer period if this thought to be necessary as part of further investigation and measures that may be taken against the user by the competent authority or judicial authorities. As soon as a further investigation has been closed or the competent authority (or if relevant, the judicial authorities) believe that there is no reason or insufficient reason to take measures with respect to a user, the information will be discarded.
- 5) The information obtained from monitoring will be retained as long as this necessary as part of a further investigation and possible measures to be taken as referred to in 11.4. As soon as this further investigation has been completed or if it does not lead to measures with respect to a user, the information, including the investigation records, will be definitively discarded.

Section 12 Right to inspection

- 1) The user has the right to inspect the information as referred to in Article 7.
- 2) Requests for information as referred to in Section 35 of the Personal Data Protection Act and requests to report provision of information to third parties as referred to Section 32 of the same act will be addressed to the Director of the Facilities Service.
- 3) Requests for inspection will be decided within two weeks.
- 4) The Director of the Facilities Service is authorised to deny a request for inspecting information based on the grounds referred to in Section 43 of the Personal Data Protection Act.

- 5) The Director of the Facilities Service can require the individual making the request to appear in person before an individual designated by the Director and identify himself or herself.
- 6) If desired, the individual making the request is provided with a copy of the information requested.

Section 13 Right to correction

- 1) The user has the right to correct and/or remove information concerning him or her as referred to in Section 7 if this information is factually incorrect.
- 2) Requests for correction as referred to Section 36 of the Personal Data Protection Act will be addressed in writing to the Director of the Facilities Service stating the desired correction.
- 3) Decisions about requests for correction will be made within two weeks.
- 4) After granting such a request, the correction will be completed within two weeks.

Section 14 Legal protection

Decisions such as those referred to in Sections 5, 12 and 13 are defined as resolutions according to the terms of the General Administrative Law Act. The objection and appeal possibilities offered by this Act therefore apply.

Final provisions

Section 15

Every year, the Director of the Facilities Service makes an anonymised report to the Executive Board and the co-management bodies about the cases where monitoring has taken place.

Section 16

The Director of the Facilities Service is responsible for making sure that, with respect to the technical and organisational security of the processing, sufficient measures are taken so that the confidentiality of the processing and the compliance with these regulations is assured.

Section 17

These regulations take effect after approval by the Executive Board of WUR and after approval by the Central Employees Council and the Student Council.

Section 18

These regulations can be referred to as the "Privacy Regulations for Network Use at Wageningen UR".

These regulations will be available for public inspection at the personnel offices of the Expertise Groups and at the Administration Centre of Wageningen UR. The text of these regulations will also be published on the Intranet of Wageningen UR. A copy of the regulations will be sent to the Registry Office.

Wageningen UR, November 2003

Code of behaviour for the use of network facilities,

specifically e-mail and the Internet

In our society, the use of computer facilities – including e-mail and the Internet – has expanded enormously. At Wageningen University and Research Centre (Wageningen UR), computer facilities are also being used on a major scale.

This code of behaviour has been established to promote the businesslike and efficient use of computer facilities. Among other things, this code provides details concerning a mutual agreement between Wageningen UR and the user including the rights and obligations related to the use of the facilities.

In consultation with the Executive Board, the Central Employees Council and the Student Council, the following rules have been established.

- 1) The computer facilities that are made available to the user, which also include the account and e-mail address (first name.last name@wur.nl), are the property of Wageningen UR or of an affiliated service or institution. These facilities are available to the users for businesslike aims concerning education and research. Every user is responsible for these facilities being used primarily in a businesslike fashion and makes sure that this use is not in conflict with any statutory provision. The user can be called to account by other individuals regarding this responsibility, specifically by his or her superior or, in the case of a student, his or her study supervisor.
- 2) With due regard for businesslike use, it is permissible to use electronic mail and access to the Internet for private purposes if this use is limited and in good taste and does not disturb the activities of other users.
- 3) The link of Wageningen UR with the Internet proceeds via SURFnet. This organisation permits use of its facilities only for education and research. Private commercial activities are forbidden.
- 4) Both the businesslike and private use of the computer facilities of Wageningen UR must satisfy at least the following preconditions:
 - a. it is not permissible to provide unlawful access to software, computer files and computer facilities, or undertake attempts to this end;
 - b. it is not permitted to deliberately visit Internet sites that contain pornographic or racist material, or sites with degrading or offensive content;
 - c. if the user accidentally encounters such a site, he or she must leave the site immediately;
 - d. it is forbidden to distribute pornographic or other sexually-oriented material, or material that is racist or otherwise insulting, hurtful or damaging to the reputation of Wageningen UR or others, by e-mail or other forms of electronic communication;
 - e. it is forbidden to send e-mail for private purposes to large groups of users, including chain letters and comparable documents;
 - f. it is forbidden to download illegal software and other illegal files, to save them, to use them and/or to distribute them;
 - g. it is forbidden to use information for any other purpose than that for which it is intended;
 - h. the computer facilities provided must not be used for personal gain.
- 5) Viruses are a serious threat to computer facilities and the information and documents present on these facilities. Every user must therefore take precautionary measures to prevent the introduction or spread of viruses. E-mail and other files that are sent or received via the network or another medium must be scanned for viruses before they can be opened, saved or distributed on the computer facilities of Wageningen UR. Should the occasion arise, the user must report any suspicion of the presence of a virus to the local system administrator.
- 6) Users of the computer facilities of Wageningen UR are always responsible for all activities that take place via their personal network access – comprised of a user name and password. They are therefore responsible for keeping their password confidential. Consequently, users should never print passwords, make note of them or make them available to someone else. A user can make

use of the network access of another individual only if he or she has given express permission for this.

- 7) The network administrator of Wageningen UR has the right to collect and analyse information concerning network use. This information can be used to determine which Internet sites have been visited from Wageningen UR. This concerns information that cannot be attributed to an individual.
- 8) If there are already indications of network use that is in conflict with the code of behaviour, information that can be attributed to a single individual can be registered and examined. In that case, the "Privacy Regulation for Network Use at Wageningen UR" applies. This regulation is included in the Student Charter and is available for inspection at the HRM office of Wageningen UR, the personnel offices of the Expertise Groups and on the Intranet of Wageningen UR (WURweb).
- 9) If there is a violation of the provisions in this code of behaviour, suitable measures can be taken by Wageningen UR against the user. Depending on the seriousness of the violation, this can lead to the revocation of network access, termination of employment and/or filing criminal charges with the judicial authorities.
- 10) The network administrator of Wageningen UR has the right, from a technical or functional point of view, to indicate specific links on their network as undesirable and to have them closed.
- 11) Disputes emerging from the application of these regulations can be presented to the relevant regular grievance committees within Wageningen UR.

Wageningen UR, November 2003