REGULATIONS FOR THE USE OF COMPUTER SYSTEMS AND COMMUNICATIONS NETWORK - NETIQUETTE -

CONTENT

1. Regulations for the use of computer systems and communication network at Karelia University of Applied Sciences
2. Acceptable use of FUNET and allowed network connections
3. Students’ access rights in computer systems
4. Data security and responsibilities
5. Regulations for the use of University of Applied Sciences information systems for maintenance staff

REGULATIONS FOR THE USE OF COMPUTER SYSTEMS AND COMMUNICATIONS NETWORK AT KARELIA UNIVERSITY OF APPLIED SCIENCES - NETIQUETTE

INTRODUCTION

1. Karelia University of Applied Sciences aims at providing the University of Applied Sciences personnel and students with an opportunity to use computers and communication networks. For guaranteeing all users the best possible working conditions, the following regulations need to be applied by all. These regulations are common to all and their purpose is to define the users of systems and the maintenance staff their rights and responsibilities.

2. These regulations apply to the use of all computer systems and communications networks administrated by Karelia University of Applied Sciences and to other systems used by the authorisation of University of Applied Sciences Computing Services. Karelia University of Applied Sciences Computing Services and its operational activities are maintained by the Information Technology Service Centre of the City of Joensuu, referred to as maintenance staff/administrators later in this text.

3. Similar regulations for the acceptable use of computer systems and communications network and for user ethics are applied in many other organisations belonging to or connecting with University of Applied Sciences data processing systems. These organisations in-
clude FUNET, Nordunet, and NSFnet in the United States, for example. Corresponding regulations for other Finnish Institutions of Higher Education, such as University of Helsinki and Helsinki University of Technology, have been adapted when compiling these regulations.

4. These corresponding regulations at different Institutions of Higher Education in Finland make student mobility more fluent and facilitate problem solving between these institutions.

5. These regulations base on following general principles:
   - All users are entitled to use computer systems and communications networks in an appropriate manner.
   - Other users shall not be harmed.
   - Privacy protection shall be respected.

6. The maintenance staff reserves the right to complete these regulations with particular instructions for the use of equipment, software and networks.

OBLIGATIONS OF THE MAINTENANCE STAFF

1. The maintenance staff is responsible for arranging proper working conditions. Administrators in charge of data processing systems and data communications are responsible for the practical arrangements of maintenance work.
2. Licenses for the use of University of Applied Sciences computers are granted upon application. Entitled users include University of Applied Sciences personnel and students needing to use a computer in their studies.
3. Basic instructions concerning the use of computer systems can be obtained from Computing Services. The maintenance staff informs users of changes in the systems and of their effects on use. Furthermore, users are provided with additional information and instruction, if needed.
4. The maintenance staff is obligated to maintain secrecy.

RIGHTS OF THE MAINTENANCE STAFF

1. In order to fulfil its obligations, the maintenance staff has the right to restrict and regulate the use of computer systems.
2. Administrators in charge of computer systems have the right to examine user files in urgent fault situations within the computer system and in suspected situations of misuse.
USER OBLIGATIONS

1. In order to enable good working conditions, users shall feel responsible for the use of computer systems. These rules apply to systems requiring login (user computers and network workstations) and to those applicable parts of the system for which a user name is not required (microcomputers and data communications equipment).
2. Every user shall use his/her own name and personal user name. Exceptions are granted in cases where the use of anonymous login or pseudonyms is allowed as well as in cases where course or group user names have been given for a specific purpose. The owner of the user name is responsible for the code being used merely in accordance with the regulations issued in the license application.
3. Users shall take other users of the system into account.
4. Users shall take care of issues related to common information security. If the user himself/herself does not have anything special to protect, it might not be the case with some other user. Careful use of the password is essential for avoiding misuse. All users bear responsibility for the overall security of the system.
5. Instructions given by the maintenance staff shall be observed.

USER RIGHTS

1. The licensed users of the system are entitled to use the equipment and communications network in the ways needed, presuming that the use is related to University of Applied Sciences activities, i.e. studying, teaching and administration. Permissible use includes:
   - acquiring information in order to perform work assignments
   - developing professional competence
   - trade union activities
   - permissible private use, including only
     - banking activities
     - occasional communication and informing of urgent issues difficult to be dealt with elsewhere or in other ways
2. Users are entitled to take initiatives for the development of computer services to the maintenance staff.
3. Users are entitled to make individual complaints to the personnel of Computing Services and, thereafter, to Karelia University of Applied Sciences Management Team, if being dissatisfied with any measures taken by the maintenance staff.
RESTRICTIONS ON USE

1. Use or distribution (with online services, for example) of commercial, political, religious, ideological, immoral or other equivalent unethical material is prohibited within the system.

2. Disturbing other users either directly or indirectly is prohibited. Indirect disturbance includes, for example, any interference caused by squandering the capacity of the information systems or networks.

3. The use of University of Applied Sciences computer systems and communications networks shall be related to studying, teaching, research, or administration within the University of Applied Sciences, in accordance with the terms and conditions in the license. The use of user name for commercial purposes is strictly forbidden. Other chargeable use shall always be separately discussed with the maintenance staff.

4. Attempting to use, and the use of, any system requiring a personal user access code is prohibited, if no valid code for the person has been assigned. Attempting to access a system with an incorrect user name as well as exceeding or attempting to exceed the authorisation of a personal user access code is prohibited.

5. Connecting computers or other communication devices to the communications network without a permission given by Computing Services is strictly forbidden. Devices connected to the network shall only be used for receiving information addressed to the user him/herself.

6. Changing hardware and system software is prohibited. This rule applies also to common systems assigned for one user.

7. Evading or attempting to evade quotas or other restrictions is prohibited.

8. Seeking out or using known or new weaknesses in data security is prohibited.

9. Illegal copying of software and data is prohibited.

10. Installing software or scripts in any device possessed by Karelia University of Applied Sciences is prohibited, without a separate permission granted by the maintenance staff.

MISUSE AND CONSEQUENCES OF MISUSE

1. Misuse of computer and communications systems refers to all activities that
- interfere with the purpose for which the system was primarily procured
- cause detrimental harm or damage on the telecommunications network to which he system is connected or on any other systems connected to this network
- contravene regulations
- use such parts or features of the system that are indicated as prohibited
- are prohibited by the owner or the person responsible for the system

2. Karelia University of Applied Sciences Computing Services supervises the observance of these regulations. In cases of suspecting misuse of data processing systems and communications networks, the following procedures shall be taken:

- an administrator contacts the user, finds out the purpose of particular actions, and states his/her view on these actions
- depending on the severity of misuse, the user may be cautioned, or given restrictions or a temporary prohibition on use by Computing Services. Full prohibition on use shall apply in cases of internal misuse within the University of Applied Sciences and in cases where misuse continues despite a warning.
- assigned people in charge of the systems are, in cases necessary, entitled to prohibit or restrict the use of systems during investigation
- during investigations, the user and other parties involved must be heard. As a result of hearings, future procedures must be decided. The user has the right to complain about the decision to University of Applied Sciences Management Team.

3. The users shall note that Person Register Law, Criminal Law and Copyright Law contain regulations concerning the use of information technology.

4. In cases of severe misuse, or in cases of misuse being directed outside the University of Applied Sciences and with possible criminal offence taking place, the misuse can be handed over for police investigation.
2 ACCEPTABLE USE OF FUNET AND ALLOWED NETWORK CONNECTIONS

FUNET-project
Tietotie 6
FIN-02101 ESPOO
Markus Sadeniemi

The purpose of this memo is to define the appropriate use of FUNET-network and the acceptable network connections. Moreover, an aim is to define the procedures used to prohibit inappropriate use of the network. A data communications network is presumed to form a hierarchic structure where a number of national networks connect University of Applied Sciences or corporate networks (e.g. University of Applied Sciences campus network or localarea network for a company) to one national network (FUNET). All these networks form a Nordic NORDUnet-network connected to a worldwide network. In this memo, focus is on data communication originating in some network of FUNET’s member organisation and being transferred through FUNET to the network of another member organisation or to some other network connected to FUNET either in Finland or abroad.

Data communication must be accepted in all networks used. For example, data communication from one Finnish University of Applied Sciences to an Institution of Higher Education in the United States must follow the regulations of both institutions, FUNET and NSFnet. The regulations are, yet, usually pretty similar with each other.

1. Definitions
The purpose of FUNET is to provide University of Applied Sciences and Universities with network connections and other data communications services. FUNET also serves research institutes and companies carrying on research by providing them with communications networks needed in research work.

Acceptable use coincides with all regulations for the networks connected to FUNET. This applies both to standard applications, including e-mail, data transfer and remote login, and to exceptional use, such as testing of data communications protocols.

An acceptable network connection is a connection between networks enabling data communication through FUNET-network. The network connection should also have an appropriate license and fulfil the prerequisites for connecting to the network.

2. Acceptable use
FUNET’s objective is to do its share in promoting Finnish research and teaching at higher levels of education. The use of network supporting this statement is usually acceptable use. Thus, use
connected to chargeable service activities (i.e. research projects) in member organisations is acceptable. Instead, commercial use of the network is usually prohibited. Commercial services benefiting the research organisation are, however, possible, but a license for them must be applied from FUNET.

Examples of different types of situations of acceptable/unacceptable use are listed below:

1. All use shall follow the principles of academic goals and goals of other member organisations served by FUNET.
2. Uncommercial activity serving research and teaching is acceptable.
3. The use of the network can be acceptable also in cases where it is not directly attached to research, assuming that an indirect connection to research exists. For example, data communication serving the infrastructure of research and teaching is acceptable.
4. Commercial use of commercial companies is usually not acceptable, unless it can be justified based on the item (3) in this list. FUNET Management Team must give a separate permission for this kind of commercial use.
5. Use for research and teaching purposes in commercial enterprises is usually acceptable. Instead, administrative or operative use is prohibited.
6. The use of the network must coincide with the ethical instructions (see the appendix) and received good practises.
7. FUNET Management Team is entitled to decide whether some form of use is acceptable or not. Users and member organisation are informed of these decisions.

3. Permissible network connection
FUNET aims at taking care of that networks connected to FUNET support the efficient use of the common resource and protection against disturbances. Member organisations shall also aim at this same principle.

FUNET needs to be aware of which networks are connected to it and for which purposes the network is used. FUNET must always be informed if the network of a member organization can be used for FUNET-connections of a third organisation. Reselling of the network connection (e.g. offered by a technology park or other member organisation) is acceptable only with FUNET’s permission. Connections causing severe routing problems or connections that conflict with common efficient use of the network shall not be set up.

4. Obligations of member organisations
FUNET delivers these regulations to its member organisations, which must inform their users of them. Responsibility for the network being used in acceptable ways is primarily in the hands of the member organisation in charge of the connector’s network. In case of acceptability of use not being clear, FUNET must be contacted.
5. Implementing the use of FUNET
In cases where some type of use is considered not acceptable according to the principles of FUNET, the source network for data communication (usually a FUNET member organisation) is liable to point out the network concerned and prohibit misuse in the future. To the best of its ability, FUNET takes care of that FUNET and other networks connected to it (particularly international networks) follow the rules of acceptable use and permissible network connections. FUNET member organisations are obligated to do the same.

Ethics for the use of FUNET and other research organisations (an extract from the appendix of this memo) FUNET states as unethical and not acceptable any activity that
- aims at using network resources without permission
- is used for falsifying one’s identity, except in cases where a user is allowed to hide his/her identity
- disturbs normal operations in the network
- wastes the resources (human, network or machinery capacity)
- destroys or changes saved information without permission
- threatens the privacy of network users
- insults or significantly disturbs other users

3 STUDENTS’ ACCESS RIGHTS IN COMPUTER SYSTEMS

USER RIGHTS

User licenses are admitted by Karelia University of Applied Sciences Computing Services. A user license is always personal and temporary, with the exception of specific course and group codes. A prerequisite for receiving a user access code is following the technical and ethical regulations compiled by Computing Services in the use of computer systems.

The user verifies his/her commitment to the existing regulations with a signature. The code owner is always responsible for any measures taken under his/her code and for resources used. Handing the code over to someone else is prohibited and does not repeal the code owner’s responsibility.

Misuse of the computer system and communications network may lead to partial or total loss of user rights. In cases of severe misuse, or in cases of misuse being directed outside the University of Applied Sciences and with possible criminal offence taking place, the misuse can be handed over for police investigation.
Karelia University of Applied Sciences Computing Services is entitled to remove user rights without any notice immediately after the student has finished his/her studies.

**USER NAMES**

The system serves individual students in their studies and research. A prerequisite for getting a user access code is getting acquainted with the computer system and being familiar with the regulations for it. Furthermore, the student must have a valid right to study. A user name is granted by Karelia University of Applied Sciences Computing Services and it is usually applied for through HelpDesk. More information is available at [http://www.karelia.fi/](http://www.karelia.fi/).

**USERS**

User rights for the above-mentioned systems can be granted for all students at Karelia University of Applied Sciences and also, within certain limitations, for students at other University of Applied Sciences and Universities.

**MAINTENANCE STAFF**

Karelia University of Applied Sciences Computing Services is in charge of the communications network and the resources connected to it. Computing Services aims at promoting the efficient use of the network and its resources. An objective is also to protect the network from disturbances and to follow the users’ complying with the rules.

**4 DATA SECURITY AND RESPONSIBILITIES**

Everyone shall be involved in common data security, since all users are responsible for the overall security within the information system. A user name and its related password are personal and should not be disclosed for use by others. This applies to course codes and their passwords, too. Any password that may have been disclosed to a third party must be changed immediately. In any case, the password needs to be changed at certain intervals.

Each user is responsible for all activity occurring under his/her user name. The systems are to be used with great care and in accordance with good practises. For example, when using systems requiring login, logging out is required as well. Users shall note the fact that legislation, including Telecommunications Law, Person Register Law, Criminal Law and Copyright Law, for exam-
ple, contains regulatory provisions on the use of information technology. A claim for damages, fines or even imprisonment can be allocated at a person offending.

Seeking out and reading data regarding or belonging to another person is permissible only with his/her permission. Should a user come into the possession of data addressed or belonging to others, its use, storage or circulation is prohibited. In this case, both the appropriate user and maintenance staff shall be informed.

Each person shall always use only his/her own name and user name, except when using course codes for specific purposes or pseudonyms in newsgroups, for example. Course codes shall not be used outside courses. Communications networks to other systems outside the University of Applied Sciences may only be taken by using a personal user name. The falsification of identity is prohibited. The teacher is responsible for codes used in his/her own courses and for removing them after the course.

A user shall take other system users into consideration. Moderation shall be observed when using the University of Applied Sciences and external communications systems. Although aiming at maintaining a high level of usability and security of data systems, not all failures in operations and not all misuse of data systems can be avoided. Karelia University of Applied Sciences does not guarantee the security and confidentiality of information systems, or data integrity. The responsibility for storing research and other data ultimately rests with the owner of the material. Karelia University of Applied Sciences is not responsible for any possible damage or loss resulting from the use of Karelia University of Applied Sciences information systems.

5 REGULATIONS FOR THE USE OF UNIVERSITY OF APPLIED SCIENCES INFORMATION SYSTEMS FOR MAINTENANCE STAFF

1. Introduction
Karelia University of Applied Sciences Computing Services is the main user of computer systems and has, therefore, "full rights" to read the contents of any file without breaking encryption, and also to start or finish any programme, and to follow all processes and data communication going on. Since the rights for the maintenance staff in the administered environment are practically unlimited, they, in principle, contradict with users’ basic rights and with privacy protection. Therefore, each administrator is liable to follow these instructions where good ways of action for the maintenance staff are defined.

2. Professional secrecy
The maintenance staff shall not reveal to outsiders any information gained through his/her position and shall not, thereby, use the information for purposes not related to his/her work as an administrator. In particular, the maintenance staff is committed not to reveal to anyone any private information of users gained by the position as an administrator.
3. Respecting privacy
When working with University of Applied Sciences information systems, the civil right for privacy and anonymity in communication shall be taken into account. The University of Applied Sciences, however, reserves the right to define, which kind of material can be stored and for which purposes within the information systems administrated by it. The same applies to data communications within the communications network administrated by the University of Applied Sciences.

4. Handling e-mail messages
The main principle for handling e-mails is that the privacy of correspondence with private emails and other electronic communication is infrangible. An e-mail message is confidential, unless it is meant for common use. Should a user come into the possession of a confidential e-mail addressed or belonging to others, he/she shall not reveal the content of it to anyone, and nor can he/she use the content of the message in any way.

Confidential e-mail messages are never allowed to be read without permission. Since confidential e-mails are difficult to separate from non-confidential messages, the principle to follow is that another person’s e-mails cannot be read without his/her permission. Users’ e-mail boxes can be accessed in following cases:

- The user has given permission for it.

- An e-mail message in the post system ready to be delivered may need to be opened in cases where the post system cannot deliver it further due to its inadequate or damaged structure or content. In this situation, the main user cannot familiarise him/herself with the content of the message. The sender or receiver’s address, identity or other relay may, however, need to be checked in order to correct the situation. Handling spams is in most cases harmful for the University of Applied Sciences capacity. Spamming is hedged against with the required means, including the mail server denying accepting messages from certain servers or other e-mails filling certain criteria. This procedure may be useful for protecting users and systems, although users’ right for free emailing communication is restricted then. After the e-mail message has been received and removed from inbox, it has the same protection as any other file under a certain user name. University of Applied Sciences regulations for the use of e-mails are defined in more detail in the document “E-mail policy at Karelia University of Applied Sciences”.

5. Handling other files
The maintenance staff has no common right to read or in any other way handle the contents of other users' files, unless they are not protected. An administrator has, however, the right to handle files in following cases:

- The user has given permission for it.

- There is a justified reason to doubt that the user account has been accessed by another person, or there are files or programmes under that user name that may cause danger or threat to the capacity or security of the University of Applied Sciences. In this case, the owner of the user name will be contacted at first. However, in cases of immediate threat, measures may be taken already before the user has been contacted.

- There is a justified reason to doubt that the owner of a user name has misused the system him/herself, or it is assumed that there are specific files under that user name that have proof of misuse. Then, the maintenance staff shall report his/her suspicion and the grounds for it to the other administrators of the same system, to the person in charge of data security in his/her unit, and finally to Data Security Manager.

- A user identification possesses programmes, scripts or configuration files causing severe disturbance within the system. Then, the maintenance staff has the right to check the contents of the particular file and prohibit it from working, in case needed. This kind of a procedure must be informed to the other administrators of the same system and to the owner of the file. Users' home directories include a number of configuration files directing the operations of other programmes. This kind of files may need to be changed as a part of normal maintenance work. In addition, configuration files for certain programmes need to be read by the maintenance staff as a part of normal security surveillance. Temporary files located in the Temp-directory in the system and in user's home directory may be deleted as a part of normal maintenance of disc space.

6. Monitoring directories and file listings
The maintenance staff cannot totally avoid taking and seeing file listings in users’ directories in normal maintenance work. Handling directory structures, and names, dates for updates, sizes, levels of protection, and other information of certain files is a part of normal maintenance work.

7. Monitoring programmes, processes and data communication
The maintenance staff monitors the executable programmes within the information systems as a part of normal maintenance work. If a process is causing problems or excessive loading to the rest of the system, or contradicts with the regulations compiled by Computing Services, it can be taken off by the maintenance staff. Measures of this kind are informed to the user. If a fault or
severe loading disturbing the capacity of the University of Applied Sciences communications network is monitored, the data communication can be prohibited by the maintenance staff.

8. Handling log files
Most University of Applied Sciences information technology systems store different kind of log information of measures taken by users and of all accesses into the system. Logs of this kind are necessary when faults in the system as well as misuse need to be clarified. Most log files are protected from outsiders so that only the maintenance staff can monitor them. Many ancillary services of the mainframe, however, show information on user names to other users too.

The maintenance staff uses several log files as a part of normal maintenance work. Monitoring logs is process and computer oriented and the activities of a single user are not normally monitored. Detailed log information is handled in a confidential manner and no information of them will be revealed to any outsider. There are, however, two exceptions of these regulations:

- If the police authorities ask for delivering log files, they will be delivered to the extent required by the police authority, defined by the law on coercive means, or by court order. The assignment will be registered.

- When preventing burglars from accessing the systems and trying to hedge against breaking into the data system or against other illicit use, cooperation between other University of Applied Sciences or service providers may take place in order to clarify the origin of the burglar or isolating him/her. In this case, it may be necessary to hand over information on particular user names. This is, however, limited to user names which can fairly be assumed to be in the possession of a non-licensed user, or to user names the owner of which can be assumed to have committed a crime him/herself.

9. Monitoring network loading and possible limitations for data communication
Normal monitoring of loading only includes the amount of transferred information, not the content. This monitoring is usually computer-specific, i.e. no user information is seen as such. When monitoring loading, the maintenance staff cannot, however, avoid seeing the position of the sender and the receiver within the network as well as the protocol of this communication. The other party in the communication and the protocol are normally not stored in the logs, but they can be seen and they may be stored when investigating disturbances in the system.

When monitoring loading and data communication, the maintenance staff can see the data on the sender and receiver’s Internet addresses and on data communication protocol. Activities of a single user are not usually monitored; it is only allowed when investigating disturbances. In prioritising or limiting data communication, the regulations and recommendations of FUNET are applied.