IT Service User Rules in Brief

These binding rules apply to all users, including you. These rules apply to the use of all IT services, hardware, software and networks of the university of applied sciences.

The UAS authorises users to access its IT services by granting user IDs or making the service available. Each user is personally responsible for all use of the services with his/her user ID.

The provided IT services are intended for work- and study-related use. The services may also be used for personal purposes within reason and in keeping with laws and good practices.

Other users' privacy and ownership of information must be respected at all times. Use of the services for any commercial or propagandistic purposes is forbidden.

All unauthorised use is forbidden. The use of services is monitored and the breach of these rules will be sanctioned.

Further specifications to these rules are provided below:

IT service user rules

These IT service user rules bind and obligate all members of the UAS community, users of IT services and systems, and all units within the UAS.

The rules apply to all UAS hardware, IT services and the use thereof, also including the services made available or authorised by the UAS. Examples of such services include CSC's services HAKA, Funet etc.

Terms of Use for Cloud Services at Karelia University of Applied Sciences are valid and can be found via this link. (Approved 14.3.2016.)

Data and privacy protection principles for **learning environments** (such as Moodle) of Karelia UAS are the same as for email system of Karelia UAS from the beginning of August 2016. Accordingly when there is need to change or add access for faculty or staff into cources in learning environments, the rule for Retrieving and Opening an Employee's Email must be complied with. Link to this rule may be found by this.

Usage authorisation

Usage authorisation is granted by issuing a user an ID or making the service available.

Authorised users have the permission to use the IT services provided by the UAS. Compliance with these IT service user rules is a prerequisite for the authorisation.

– the scope of usage authorisation depends on the user's status and duties (roles) at the UAS
– a person may have several roles at the same time

Usage authorisation is temporary

The authorisation expires when

- the person is no longer a member of the UAS community as a result of termination of employment or right to study
- the granted fixed term user ID expires
- the person's role changes and the new role does not make him/her eligible to use the IT service

Usage authorisation can be restricted if there is a justified reason to suspect that information security has been compromised or the services have been abused.

The user needs to remove all personal emails and files from his/her email account before the expiry of his/her usage authorisation. The UAS will delete all files and the mailbox contents after the expiry of the user ID or usage authorisation. UAS staff members, as well as students who have worked in e.g. research teams or participated in other such activities, must transfer all workrelated messages and files to a person specified with the supervisor.

All users must uninstall any software based on employee or student licences from their home computers when their employment or right to study ends.

User ID

- a user is identified (authenticated) with his/her user ID
- each user must have an individual ID for all IT services that require authentication

Group ID can be granted upon request for a special purpose

The use of a group Id can compromise the confidentiality of information. An example of such a case: an administrator-level group ID has been granted in order to use special software in a computer lab or a common ID for an email account.

- the user applying for a group ID is responsible for the distribution of the ID
- the group ID may only be used for the purpose specified in the application and in the granted permit
- each user of the group ID is responsible for his/her actions conducted using the ID

Each user is personally responsible for his/her user IDs

User IDs must be protected using strong passwords and complying with other instructions. If there is a reason to believe that a password or other account details have been compromised, the password must be changed or the use of the compromised account must be prevented immediately.

- never dispose or lend your user ID to another person
- each user is responsible for all actions conducted using his/her user ID
- the user is financially and legally liable for any damage or loss caused using his/her ID
- the use of another person's user ID is forbidden, even upon the user's own request

User rights and responsibilities

IT services are intended for work- and study-related use

The UAS IT services are intended to serve as tools in tasks related to UAS studies, teaching, research or administration.

Small-scale private use is allowed

Small-scale private use refers to such actions as private email conversations and use of online services. However, private use must never

- disturb other use of the system, or
- breach the rules and instruction for the use of IT services.

Commercial or propagandistic use is not allowed

However, special written permission for these purposes can be applied from the Head of IT Services.

- commercial use is only allowed in cases assigned by the UAS
- use for pre-election campaigns or other political activities is only allowed in conjunction with UAS elections and activities of e.g. the Student Union, student organisations or trade unions
- all propagandistic use is forbidden
- unnecessary consumption of resources is forbidden

Laws must be obeyed

- illegal material or material that is against common manners must not be published or distributed

Each person is entitled to privacy

However, the right to privacy does not cover all work-related material that is in an employee's possession.

- all material that is in a student's possession is deemed to be private
- employees must clearly separate their private materials from work-related ones
  + e.g. create a directory entitled "Private"
  + these rules also apply to students working at the UAS

Information security is everyone's responsibility

Any detected or suspected breaches or vulnerabilities in information security must be immediately reported to the IT personnel (tietohallinto@karelia.fi).

- personal passwords must never be disclosed to anyone
- everyone is obligated to maintain the secrecy of any confidential information that may come to one's knowledge
- hacking, abuse, copying and distributing of other users' private information is forbidden

The UAS is entitled to restrict or revoke the right to use its IT services as a precaution.

Setting up an unauthorised service is forbidden

Only devices and software approved by the UAS may be connected to the UAS IT network. Only services authorised by the UAS IT Services may be produced using the UAS IT network.

Bypassing information security mechanisms is forbidden

Usage rights must never be used for any illegal or forbidden activities, such as searching for vulnerabilities in information security, unauthorised decryption od data, copying or modifying network communications, or unauthorised access or attempted access to IT systems.

Parts and features of IT systems that are not clearly made available for public use must not be used, e.g. system administration tools or functions prevented in the system settings.

Phishing for information and deceiving of users is forbidden

Cheating and unauthorised acquisition of information is forbidden.

Other regulations

Validity

These IT Service User Rules become effective as of 1 January 2014 and replace earlier corresponding rules. After the date specified above, all new IT services must be produced according to these rules.

Change management

These email rules will be reviewed when needed to ensure that they comply with all valid services and laws. Any significant changes to these rules are addressed according to the co-operation procedure. The Head of IT-Services makes decisions on any needs for change.

Information about changes is distributed using regular communication channels, never personally.

Deviations from the rules

Permission for exceptions from the rules can be granted for compelling reasons upon a written application. Exceptional permits are granted by the Head of IT-Services and they may include additional terms and conditions, restrictions and responsibilities.

Monitoring

Compliance with the rules is overseen by IT Services, owners of services and IT services as well as supervisors within their job descriptions. Breaches of these rules lead to sanctions according to the consequences of IT service abuse.

Further information

The regulations and instructions concerning IT-services can be found via this link: link to instructions
The instructions referred to or related to by these instructions are:

- IT Service User Rules (this document)
- Email Rules
- Retrieving and Opening an Employee's Email
- Consequences of IT Service Abuse
- Tables of Penalties of IT Service Abuse
- Administrative Rules for Information Systems