IT services terms of use - summary

The terms of use are binding and they must be observed by all users, including you.

The terms apply to all IT services, equipment, applications and networks of the university.

The university grants users access rights to use the IT services by issuing a user ID or by making the service available.

Each user is personally responsible for all use of the services under his or her user ID.

The IT services are intended for work and study purposes.

In addition, users are permitted to use the services for private purposes, provided that it is done within reason and in compliance with the law and good practice.

Privacy and the ownership rights to information must be respected by all users.

All forms of commercial or propagandist activities are prohibited.

Use of the services in breach of the terms and conditions is prohibited.

Use of the service is monitored and any breach may result in disciplinary action.

Terms of use of IT services

The IT services terms of use are binding and must be observed by all members of the university community, users of IT services and information systems, and all departments and units of the university.

The terms apply to all equipment and IT services of the university and their use. They also apply to services which are made available or whose use is authorised via the university. These include services such as CSC services, e.g. HAKA, Funet, etc.

The terms of use are in compliance with current legislation.

User licence

The user licence is granted by issuing a user ID or by making the service available

Authorised users have a licence to use all IT services of the university. Compliance with the terms of use of the IT services is a prerequisite for a user licence.

- User authorisations to the IT services depend on the status and duties (roles) of the user at the university.
- A person can have multiple roles simultaneously.

Authorisation is granted for a fixed term

The user authorisation expires when

- the person is no longer a member of the university (employment contract, a student, an alumnus, other equivalent member status).
- authorisation granted for a fixed term expires.
- the person's role changes to the effect that user authorisation to IT services is no longer necessary.

User authorisation can be restricted if there are reasonable grounds to suspect that data security has been jeopardised or the service has been used inappropriately.

The user must delete his or her personal email messages and files before the authorisation to the IT services expires. The university will delete files and mailboxes six (6) months after the expiry of the authorisation or later. Staff members must forward messages and files which are related to their job duties to another person as agreed with the supervisor. This also applies to students who have worked as part of research teams or in other roles.

Each user must personally remove any software which has been licensed for home use as a staff member/student benefit when his or her employment contract or student status ends.

User ID

- Users are identified (authenticated) by a user ID.
- Each user must have a unique ID for IT services which require authentication.

Group IDs can be issued for specific purposes upon application

The use of group IDs can jeopardise the confidentiality of information. Example: a group ID is issued for administration privileges required for specialist software in a computer classroom.

- The group ID applicant is responsible for disclosing the ID to other users.
- The group ID must not be used for purposes other than that for which it is intended.
- Each user of the group ID is personally responsible for its use.

Each user is personally responsible for the use of their ID

User IDs must be protected using strong passwords or by other methods as instructed. If there is reason to believe that the password or other identification has ended up in the wrong hands, the password must be changed or the use of the ID must be prevented immediately.

- User IDs must not be disclosed to other people.
- Each user is personally responsible for all use of the ID.
- The user has financial and legal responsibility for any loss or damage caused by the use of his or her user ID.
- The use of another person's user ID is prohibited even if personally requested (excluding possible IT support tasks by the data administration department).

User rights and responsibilities

The IT services are intended for work and study purposes

The university's IT services are intended for use as tools in tasks related to study, teaching, research or the university's administration.

Personal use is permitted within reason

Reasonable personal use includes, for example, personal email exchanges and the use of online services. However, personal use must not

- interfere with other use of the system, or
- violate the terms of use or other instructions issued.

Commercial or propagandist activities are not considered permissible personal use

Users may, however, request special permission from a data administration official. The permit must be issued in writing and signed.

- Commercial use is permitted for the university's purposes only.
- Use of IT services for electoral advertising or other political purposes is only permitted in conjunction with the university's elections or as part of the activities of student associations or trade associations etc..
- Any kind of propagandist activity is prohibited.
- The unnecessary use of resources is prohibited.

Laws must be observed

- The publication, distribution or dissemination of illegal or unethical material is prohibited.
- Unethical material also includes defamatory or threatening statements and bullying.

Every person has a right to privacy

Note, however, that privacy does not cover all the materials in your possession, such as those related to your job duties.

- Materials held by students are considered private.
- Staff members must keep their private content clearly separate from work-related content.
  - e.g. in a directory labelled "private".
  - this also applies to students who work at the university.

Data security is everyone's responsibility.

Any defects or abuse discovered in data security must be reported to IT administration immediately.

- Never disclose your personal password to anyone.
- Each user is bound by confidentiality with regard to any secret information to which he or she may become privy.
- 'Fishing' for other persons' information or exploitation, recording or distribution of such information is prohibited.

The university reserves the right to restrict or prevent the use of its IT services as a protective measure.

Making unlicensed services available is prohibited

Services in the university's networks may only be produced with the university's permission.

Overriding of the data security mechanisms is prohibited

No user authorisation can be used for illegal or unauthorised activity, such as scanning for vulnerabilities in data security (unless by express written authorisation), unlicensed decryption, copying or modifying data traffic, or hacking systems.

The use of any system components or features which are not clearly publicly available is prohibited.

'Fishing' and misleading users is prohibited

You must not defraud or mislead anyone to get information.

Miscellaneous

Validity

These IT service terms of use are effective from 1 January 2014 and supersede any previous terms of use.

Change management

These terms of use can be revised as necessary to meet the requirements of current services and legislation. Major changes will be reviewed as a cooperative assessment. The need for changes is determined by the manager or director of data administration.

Changes will be published through regular communication channels, not individually to each person.

Exceptions to the terms of use

Exceptions to the terms of use may be granted by written application and on specific grounds only. Exceptions can be granted by the manager or director of data administration. Special permissions can be subject to conditions, restrictions or additional liabilities.

Monitoring and control

Compliance with the terms of use is monitored by the data administration department, the owners of services and IT services, and individual supervisors as part of their duties. Violations will be handled in accordance with the disciplinary procedure for IT violations.

Further information

Rules and guidelines related to IT services are available on the university's Intranet. The relevant guidelines related to or referred to in these terms of use are:

- This document
- Email policy
- Disciplinary procedure for IT violations