Contents:

1. Purpose of the rules

The Seinäjoki University of Applied Sciences and the Seinäjoki Vocational Education Centre maintained by the Joint Municipal Authority for Education (maintenance organisation) is a scientific and research community and a public body providing basic vocational education and adult education and taking care of the official functions of apprenticeship training. It must safeguard the confidentiality, integrity and availability of all the data of its user groups, and offer a reliable and secure environment for data processing. These and other rules have been drawn up to help the users of different groups to identify the rights, responsibilities and obligations related to their user rights. Even the unintentional neglect of obligations concerning user rights may jeopardise the integrity, confidentiality and availability of data owned by other users.

These rules will be applied to all data systems and the use of all data systems under the control of the maintenance organisation or otherwise the responsibility of the maintenance organisation, and, as far as users are concerned, also to other services the possibility or right to use of which is granted by the maintenance organisation. The rules also concern work stations in general use within the maintenance organisation and all equipment connected to the organisation's network.

Corresponding rules concerning acceptable use and user etiquette are in force in many other communities, some of which the data processing systems of the maintenance organisation can interpret or some of which they are connected to such as FUNET, NORDUnet, etc.

All users of the maintenance organisation's information technology must observe not only its operating rules but also other rules and guidelines issued concerning the organisation's data systems, best practices and Finnish law.

The most up-to-date version of the rules can be found at the website of the maintenance organisation: http://www.epedu.fi/kayttosaannot/.

2. User principles

The general key principles guiding all use and the interpretation of all user rules are as follows:

- All authorised users may use the system in a moderate and practical way.

- It is not permitted to cause inconvenience or damage to other users or to other organisations or data systems in the communications network.
- The protection of privacy must be respected.
- The user rights granted by the maintenance organisation are non-transferrable.
- The user is responsible for all use of his/her User ID.
- The data systems of the maintenance organisation are meant to be used as a tool for tasks concerning study, research, teaching or administration within the organisation. Use for other purposes requires a special agreement.

The use of the maintenance organisation's data systems, data networks and the communication they carry such as e-mail must concern teaching, study, research, administration or other work related to the organisation. Use for any other purpose is possible only if authorised by the faculty, and taking into account other restrictions of use. In order to ensure the protection of privacy, private material must be kept clearly separate from work-related material. Use for political activity (such as election advertising) is forbidden. Exceptions to this are the election of the board of the maintenance organisation and the activity of the student union (student political organisations/associations) and staff trade unions.

All users must take care of matters related to common data security. Even if one user does not have anything special to protect, other users might. All users must bear their share of responsibility for the overall security of the data system. If a user notices or suspects a deficiency in or abuse of data security, he/she must notify the Dean of his/her faculty, the person at the faculty in charge of computers, the Senior Systems Analyst in charge of data security or IT Manager.

The maintenance organisation will endeavour to protect all users from malware, junk e-mail and from attempts to infiltrate the systems or individual work stations. Users too must ensure that they participate in this activity in accordance with the given instructions.

The users themselves are responsible for the protection of their files and for making back-up copies of them. The maintenance organisation will make back-up copies of the files in the centralised data systems, but are not liable for damages caused by the possible destruction of such files. Neither is the maintenance organisation or persons in charge of computers liable for damage or loss suffered by users, which results from the use of the organisation's data systems.

Users are obliged to keep secret the data contents of the systems, as well as their methods of use, levels of security and properties, whenever the purpose of the systems, the regulations concerning their use or legislation require it.

Only equipment approved and registered by a network administrator may be connected to the network of the maintenance organisation. When connecting, the given instructions must be observed.

3. Classification of maintenance organisation data systems

In order to maintain confidentiality, the data is classified into three data security classes: confidential, internal and public data (table below shows classifications of maintenance organisation data systems). Confidential data is only available to those authorised to use it. Internal data is available to those within the maintenance organisation. Public data is freely available to all. The maintenance organisation's data systems are only for the use of those who have been authorised by the maintenance organisation.

Data systems	Data classification
Maintenance organisation network management system	Confidential data
Maintenance organisation website	Public data
Maintenance organisation Intranet/Extranet	Internal data
Video conferencing and video teaching	Confidential data
E-learning systems	Internal data
Maintenance organisation's own library databases (CD-ROM)	Internal data
E-mail and directories	Confidential data
Toolkits, teaching software	Internal data
Winha student administration and its different parts	Confidential data
Winha student interface	Confidential data
Library production database	Confidential data
Library web-based database / view	Public data
Financial and human resources administration	Confidential data
Case management / Municipal office	Internal data
External human resources registers	Confidential data
External production of data and statistics	Internal data
Internet	Public data

4. Rights of administrators

The administrators of the maintenance organisation's computer systems (persons responsible for maintenance) are authorised to monitor, restrict and regulate the use of the computer systems and communications network, and, if necessary, to copy, transfer, delete or read data in computers or networks.

If the connections become overloaded, too expensive or their use causes security risks, the administrators may restrict communications.

The administrators have the right to read or otherwise interfere with user files and network traffic without the permission of the user only if the solution of a system malfunction requires it or there is reason to suspect misuse or illegal use of the system.

Such interference may only be targeted at those files or network traffic or part thereof, which can be assumed to affect system operation or can be assumed to be related to the case of misuse in question.

Measures taken must be registered and made known to the appropriate parties. Cases of misuse must be reported to the faculty management and to the IT Manager of the maintenance organisation.

5. Obligations of administrators

The maintenance organisation takes care of the organisation of good working conditions and appoints persons to be in charge of maintenance. A list of responsible persons must be available to users.

The maintenance organisation must ensure that the system user regulations and related instructions are available. The basic guidelines must also be available in written form.

Administrators must ensure that the effects of changes made to the systems are communicated and, if necessary, sufficient guidance concerning them is issued.

Administrators have an obligation to secrecy in relation to confidential data. No data received in connection with the monitoring or administration of system use may be misused.

6. Rights of users

Students and staff of the maintenance organisation have the personal right to use the IT services of the organisation for tasks related to the activity of their faculties. Use for other purposes requires a separate agreement.

Legislation concerning professional education does not ensure that students have unrestricted and free-of-charge user rights to computer equipment and internet connections. Use required for studying for a degree is free-of-charge.
Users may make a suggestion concerning the improvement of the computer services of the maintenance organisation.

A user may make an itemised, written complaint to faculty management or to the IT Manager of the maintenance organisation, if he/she is dissatisfied with measures taken with regard to him/her by administrators.

7. Obligations of users

These rules concern all systems, the use of which requires user log-in and, to some extent, systems that do not require it.

All users must bear their share of responsibility for the overall security of the system.

In order to enable good working conditions, users must be aware of their responsibilities concerning system use and must take account of other system users. Users must take care of matters related to common data security.

User ID’s and passwords are non-transferrable and each person must always use their own name and own User ID. Exceptions are cases where anonymous use or use of a pseudonym is specially permitted, or course or group User ID is issued for a certain purpose.

User ID's, passwords and keys related to user permission must be handled with care to avoid misuse.

If a user accidentally receives data directed at or belonging to someone else, the exploitation, retrieval and dissemination of such data is forbidden. Such an event must be notified to administrators or to the relevant user.

Moderation must be observed in the use of maintenance organisation data systems and external communication connections.

Instructions issued by persons responsible for maintenance must be observed.

8. Restrictions on use

The unauthorised use of material that is commercial, political, religious, ideological, immoral or otherwise considered to be contrary to good practices is forbidden, as is the unauthorised use of material protected by copyright, and the dissemination of data in the system (e.g. through the internet).

The disturbance of other users is forbidden. Both direct and indirect disturbance is forbidden, for example disturbance causing wastage of capacity in the data systems or networks.

The use of systems requiring personal User ID and attempts at such use are forbidden for those who do not possess such ID. Trying to gain access to the system using false ID, exceeding the authority of a user's own User ID or attempting to exceed it are forbidden.

The transfer of User ID's, passwords and keys to a third party is forbidden.

The resale or transfer to a third party of system resources is forbidden.

The circumvention of quotas and other user restrictions or attempts at such circumvention is forbidden.

The unauthorised change of equipment and system software or attempts at such change is forbidden. This also concerns the systems of an individual user that are in common use.

The installation of software for personal use without administrator's permission is forbidden.

The search for and use of known or unknown data security weaknesses is forbidden without the special permission of a system administrator.

Use of the data systems and data networks in order to break into other systems or attempts at such a break-in is forbidden.

Operating practices generally considered to be unsuitable by the international web-based community, including SPAM, chain letters and the spreading of computer viruses are forbidden.

The unauthorised copying, possession and dissemination of software, files and other documentation (e.g. material protected by copyright) is forbidden.

If necessary, changes and additions may be made to these computer and communications network operating rules.

9. Misuse and its consequences

'Data system misuse' means all activity, which

- disturbs the use of the system for its actual purpose,
- causes inconvenience or damage within the communication network, to which the system is connected or in another system connected to the network,
- contravenes valid rules
- uses parts or features of the system, which are clearly not intended to be permitted for general use

Administrators will monitor the observance of these rules and, if necessary, interpret them. Administrators have the right to prevent or restrict use of the systems during times of investigation. In addition to this, the following measures can be initiated:

- warning
- restrictions or (temporary) ban on use
- internal disciplinary procedures in the maintenance organization
- payment based on the price list for the misuse of resources and the charging of costs arising from the investigation of misuse
- the passing of the matter over to the police for investigation and liability for the costs of court proceedings.

A user may make an itemised, written complaint to faculty management or to the IT Manager of the maintenance organisation, with regard to action targeted at him/her.

If necessary, changes and additions may be made to these operating rules.