- Never leave a laptop computer or mobile phone in a visible place in a car or leave it in a car overnight.
- Keep your desk top clean and tidy. Never leave visitors unattended or unsupervised in your office or anywhere else on the premises.
- If the memory storage tool you are using (disk, CD, etc.) suffers damage, dispose of it in a reliable way. Damaged or broken storage tools must be sent to a collection point for data protection waste or be physically destroyed.

PERSONAL INFORMATION & PRIVACY

- It must be remembered that private files stored in the data systems of the Joint Municipal Authority can also be transferred to back-up copies.
- The user him/herself is responsible for handling the personal messages that he/she receives.
- Detailed log data concerning the use of the systems is stored in the systems and data network equipment. Such data is used in maintenance, fault-finding and data security monitoring.
- All employees have an obligation of secrecy concerning private massages that come to their notice.

INTERNET AND E-MAIL

- Internet and e-mail is primarily meant to be used for work/study.
- Only use services that you consider to be trustworthy.
- Remember that you are appearing on the data network as a representative of the Joint Municipal Authority.
- It is not permitted to transmit confidential data over the internet without the appropriate encryption.
- Do not use or install on the Authority's computers software downloaded from the internet or acquired from elsewhere. Only the IT department can install software on the Authority's computers.
- Work-related e-mail is received into the e-mail system of the Joint Municipal Authority. Do not direct it outside the Authority's e-mail system. Only the IT department may carry out possible redirection. In cases of redirection, a back-up copy must always be left on the Authority's server. The user him/herself is responsible for the security and confidentiality of e-mail that is redirected elsewhere.
- E-mail attachments may contain harmful malware (viruses, worms or trojans). Beware of all unusual e-mails and particularly those with attachments. Never open an attachment from an unknown sender. Always report anything suspicious to the IT Department.

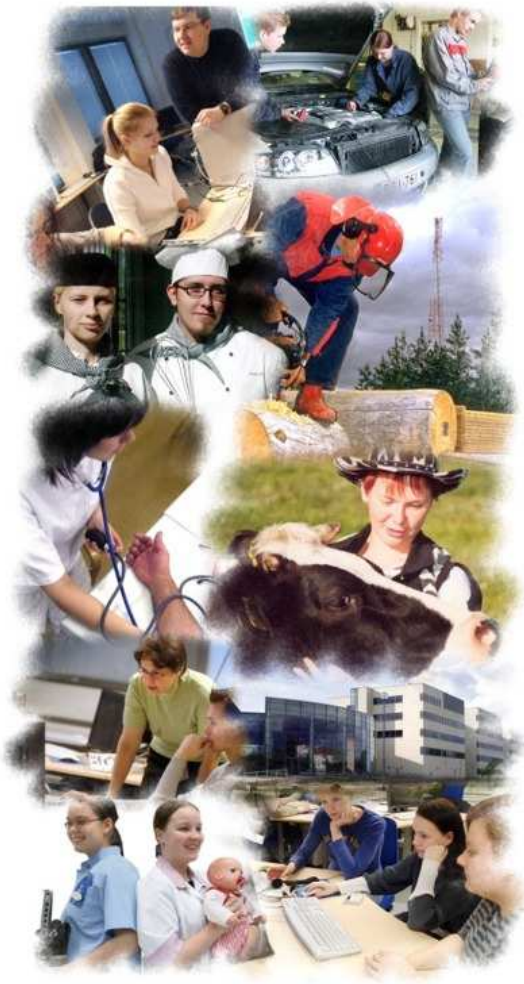
- Always maintain a healthy suspicion of e-mails; anyone can send e-mails under another name (including viruses).
- The distribution list is a list of persons, each one of whom is a recipient of the information in the e-mail. If necessary, use the hide function if you want to prevent inappropriate use of the list. The distribution list is private and confidential, and therefore the further disclosure of it is prohibited.
- At the termination of employment, your User ID will be deleted. Redirect your official e-mail to your employer and delete any possible personal messages.
- The User ID of students will also be deleted, once studies have been completed. Delete any possible personal messages.
- If you are away for a long time, agree with a colleague on the handling of your e-mails.

OBLIGATION TO REPORT

- Always immediately report malware (viruses, worms or trojans) and other matters affecting data security to the data security manager, class supervisor, teacher, IT Department or your supervisor.
- Also report immediately about any safety-related issues to the class supervisor, teacher or your supervisor.

FURTHER INFORMATION

You can get further information and help in case of problems from the IT Department in your own faculty.



SeAMK and SEDU IT security guide

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

sedu

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES
SEINÄJOKI VOCATIONAL EDUCATION CENTRE

WHY IS DATA SECURITY IMPORTANT?

The Seinäjoki Joint Municipal Authority for Education handles a great deal of confidential data, such as personal information, financial data and the student register. This data must not unintentionally fall into the wrong hands. Public information too must be handled carefully so that it is suitably available and cannot be changed without permission.

The reliable operation of data systems is crucial to the activity of the Seinäjoki Joint Municipal Authority for Education. Information issued by the Joint Muncipal Authority must be reliable. The best protection against malware (viruses, worms and trojans), data trespass and and malicious damage is the careful maintenance and use of all systems.

The greatest data security problems are usually a result of carelessness, lack of understanding and lack of expertise.

Data security is only as strong as its weakest link – not just with regards to technology but also our everyday operating practices and attitudes. Taking care of data security is the duty of every member of staff and every student. The foundation of data-secure operations is set out in the Seinäjoki Joint Municipal Authority for Education policy on data security.
http://www.epedu.fi/kayttosaannot/

COMPUTER USE

- As a user, you are responsible for your own computer. Be careful – From your computer, you can access information, which is more valuable than the device itself.
- Only the IT Department can install equipment on the network
- Only the IT Department can establish servers on the local area network
- The IT Department is responsible for installing software
- Do not change the user rights of folders and disks, so that maintenance work by the IT Department is hampered.
- Prevent unauthorised access to data systems by always locking your computer when you leave the room (press Ctrl-Alt+Del and select 'Lock computer') or log out.

USER RIGHTS AND PASSWORDS

- User rights are always needed to use the data systems.
- Never divulge your personal User ID and password to anyone else, not even to someone claiming to be a representative of the IT Department.
- Change your password sufficiently often, and immediately if you suspect that it has been revealed.
- Never let a third party use your computer, unless you can be as responsible for it then as you are when using it yourself.
- Never write down your password – at least in a place where it is easy to find.

HANDLING DATA

- Handle data carefully irrespective of whether it is on computer, paper, telephone or fax.
- Save the work that you do on the server where the information can be safeguarded by the IT Department. Check from the IT Department of your faculty what the practice is in making back-up copies of private files. Practice varies between faculties. The users themselves are responsible for the protection of their files and for making back-up copies of them.
- Check disks, CDs and other memory storage tools brought in from outside the premises using a virus protection software. The IT Department can provide virus protection software even for PCs.
- When you are travelling, only carry with you the amount of documentation that you absolute need. Never leave it unattended.
- Read instructions concerning data classification and processing at http://www.epedu.fi /kayttosaannot/
- Never let anyone see your computer display or keyboard when you are handling sensitive material or entering passwords.
- Pick up your print-out from a network printer as soon as the printing is complete.
- Use shredders or collection points for data protection waste to destroy confidential or sensitive material.
- If you have to send confidential information by fax, make sure that the recipient is standing by the machine at the other end, and that the message actually reaches its destination.

PHYSICAL SECURITY

- Pay attention to who is coming and going at the department. In a friendly way, direct visitors and people who are 'lost' to the right place.
- Never admit unauthorised persons onto the premises.
- Take responsibility for your own visitors and their movement within the department, either by yourself or with the assistance of another member of staff.
- Keep data and equipment safe.
- Never leave a laptop computer or mobile phone unattended. Keep equipment in a locked place. Also remember to keep disks, paper print-outs, etc. in a way that prevents them from falling into the wrong hands.