Title	**Guidelines for the use of ICT equipment for students at Nord.**
Owner	**Computing and IT manager**
Approved by	
Basis	
Effective date	
Archive reference	

Contents

1. General

This document sets out guidelines for the proper use of Nord University's computer equipment. All questions regarding the interpretation of these principles should be addressed to IT Services.

- Computer equipment provided to the student may only be used for limited private purposes, and private data stored on the machine is not the University's responsibility.
- Computer equipment and resources may not be used commercially, or for activities unrelated to the work of the University.
- The possibility of shared use of equipment and information entails a responsibility for using the systems legally and always acting responsibly. Students at the University are expected to respect the rights of others and use the computer equipment with due consideration.

2. Information from IT

There are several information channels available from IT Services to users (Internet, e-mail, notices, support tips, etc.). We assume that all students will familiarise themselves with what is written in these channels.

3. Information security in general

All students are responsible for keeping abreast of the University's information security policies and procedures.

4. Lawful use of computer equipment and networks

Before using computer equipment (such as computers, printers, and software), individuals must familiarise themselves with the policies that apply to the use of that equipment and ensure that they have the necessary access and skills.

Loopholes in the security systems or knowledge of special passwords should not be used to destroy or gain access to computer systems that you should have access to.

It is not permitted to store, display, share, or print material that could be offensive or provocative to others, such as defamatory statements or pornographic material.

The network/Internet should not be used to transmit information (e.g. films and music) that are not job-related.

Online games/betting on the University's equipment and/or its network are not allowed. Disciplinary action will be taken if this happens.

5. Misuse of computer resources

Computer and network resources are limited. All users are responsible for using the resources efficiently, ethically, and legally. It is not permitted for individuals to load programs or to make other changes to the computer system without the approval of IT Services.

All use of computer resources must comply with Norwegian law. In particular, if a user processes personal data, they must comply with the Norwegian Personal Data Act (Personopplysningsloven).

6. Ownership

All students must comply with the guidelines associated with software and/or data, particularly licensed software and data protected by copyright.

7. Viruses and malware

All equipment (e.g. private PCs, memory sticks, external drives) connected to the University's systems must be checked for viruses and other malware at all times. If in doubt, contact IT Services.

8. Securing user accounts and data

All users are assigned a personal user account and password. The password must be kept secret, carefully chosen, and treated in the same way as your password for online banking.

If you suspect that someone else knows your password, it should be changed as soon as possible. It is not permitted to act anonymously, impersonate someone else or use a false identity.

9. Cloud services

The University uses storage within cloud services.
Student data is saved in Microsoft Office 365.

10. E-mail:

E-mail should only be sent to recipients who may be expected to have an interest in receiving it from you.
Exercise caution when opening links and attachments from people you do not usually communicate with, always check the link address before clicking, and if it is suspicious, check with the sender.

REMEMBER: STOP – THINK – CLICK

11. Disciplinary action

Nord University may respond to improper behaviour by imposing various types of sanction. This includes withdrawing access to the University's computer equipment and networks, suspension or expulsion.

The University reserves the right, without notice, to:

- Restrict users' access to computer equipment and networks.
- Inspect, copy, remove or otherwise modify any data file or system resource that undermines authorised use of the computer equipment and could cause problems for the University.
- The University also reserves the right to periodically check any system and perform the necessary controls to protect the computer equipment. The University disclaims any liability for loss of data not stored on its servers.

Serious breaches of security regulations and this policy, and any misuse, may incur criminal liability under Norwegian law. This also applies to misuse which brings financial loss or liability on the University (such as illegal copying, Internet use etc.).

If you have any doubts about your use of the resources in accordance with good practice, ask IT Services.