KUNSTHØGSKOLEN I OSLO
OSLO NATIONAL ACADEMY OF THE ARTS

Information technology rules and regulations passed by schools governing body on 28.04.2009

Under Norwegian laws and regulation KHiO has the responsibility to control risk and safely manage information and technical resources. When you are given access to these resources (information, applications and equipment), you are also given a responsibility with regard to information security. We all share a responsibility to protect the confidentiality, integrity and availability of the information we use and security of the technical equipment used.

All users of our resources must be aware of their roles and their responsibilities.

1. **Security** rules that have been implemented should be followed. I have read and understood the rules of security in this document
2. **Username**. I am solely responsible for all use made with my username. I will logging off at the end of the workday. The locking option with password activation is to be used when leaving for more than 5 minutes from the workplace.
3. **Password** identifies you as a legitimate user of your username. Password should be personal and kept confidential. When told to change your password, you will choose a password that cannot be easily deciphered by others (i.e. no names, birthdays, etc.). If others have learned your password, you should immediately change it. If you suspected misuse of your password you will notify the IT department.
4. **Copying** licensed software is prohibited, unless the company's licensing agreement with the supplier explicitly grants this.
5. **Data** is to be saved according to the following terms:
    a. Where home and shared areas are stored on network drives and where relevant permissions are given, data will be backed up.
    b. The data of private nature and data that are not meant to be shared with others can be stored locally on your own PC at your own risk.
6. **Storage media** (examples-USB memory stick, CD, disk, etc...) as well as paper documents) that contain information that is owned and/or managed by KHiO will be handle so that it does not go astray.
7. **School property.** Equipment that employees or students receive KHiO is the school's property and shall be returned when needed or is no longer in use. IT department has a local administrator account on the school computers. This account is not to be used by employees or students. Private use of KHiO equipment may only be permitted with approval from supervisor or the IT department. Use of equipment for commercial use is not allowed.
8. **Disclosure.** KHiO will only have access to your e-mail and 'private data areas "under the conditions of the Personal Data Regulations § 9-2 and the procedures for disclosure described in § 9-3. Disclosure may thereafter be made when it is necessary for the daily operations or with suspicion of serious breaches of Norwegian law. The procedures for access mean that you will be notified as soon as possible and with reasonable justification. Personal e-mail is to be stored in a separate folder in your e-mail archives. This makes work easier and it prevents access to your private e-mail.
9. **Internet** connection at KHiO can only occur via KHiOs Internet solutions. Access to the Internet is primarily used as a source of information related to your work or study.
10. **KHiO e-mail.** Sending email from your KHiO account is considered to send a letter with KHiOs letterhead. Junk mail, chain letters, etc. are not allowed to be forwarded. Sign-ups, etc. on the Internet, should not happen with KHiOs e-mail account, but can be used if necessary.
11. **Downloading of programs** is not permitted without the explicit permission of the IT department. For the sake of clarity it is pointed out that searching and downloading others material maybe in breach of Norwegian law, such as intellectual property or copyright law. All activities on KHiOs network can be logged for security reasons.
12. **Personal information** must be encrypted by the distributor.
13. **Identification of system weaknesses.**
    Employees or students will not on their own initiative, conduct monitoring or testing of potential weaknesses in KHiOs systems and/ or network, or otherwise engage in "Hacking" against internal or external systems.
14. **Private Notebooks** are not allowed on the wired internal network without approval from the IT department. The employee / student is responsible to ensure that the device at all times is updated (antivirus, OS updates, etc.).
15. **Use of PDAs** connected to KHiO networks (such as the synchronization to Exchange e-mail server), must be approved by the IT department. The employee / students are responsible to ensure that the devices at all times is update (antivirus, OS updates, encryption etc).
16. **Controls against malicious code.** All users should use caution when opening email from unknown sources. The use of "instant messengers (IM), and activation of links and attachments in unknown e-mails or in web pages etc... Everything that is received from an outside sources (USB memory sticks, CDs etc.) should be virus checked regardless of the sender. With suspected virus contact the IT department.
17. **Reporting.** Security incidents and suspected security violation must be reported to the IT department, supervisor, student counselor and/or the security officer (CSO).
18. **As host to visitors** that are working with KHiO and/or will be using KHiO equipment, I will insure that the vistor understands the confidentiality statement and accepted (signed) the **Data Discipline Policy**.
19. **Sanctions.** Violation of the above will result in sanctions.

I have read, understood and accept the contents of this statement. I understand that I may be held liable for violations of rules given in this data discipline policy, and that violation can have consequences in addition to the consequences for my work / study conditions. This signing is for the current Data Discipline Policy. Latest version is available on the intranet.	Name: ..... Place: ..... Date:	Signature: