BUSINESS ACADEMY AARHUS
SCHOOL OF APPLIED SCIENCES

IT policy

For students at Business Academy Aarhus

Content

Purpose of the IT policy

The culture at Business Academy Aarhus is based on quality, openness, and accountability. This also applies to IT offers and systems for the students.
The IT policy contributes to securing IT operations, and the starting point is confidence that the IT users familiarise themselves with the IT policy presented here and demonstrate common sense and responsibility when using our IT facilities.

Scope

The IT policy covers the use of all the Academy’s IT facilities, including:

- All network-based IT facilities and IT systems
- Personal IT equipment loaned by the Academy
- Private IT equipment that is connected to the academy’s IT facilities

This IT policy applies to all students at Business Academy Aarhus.

General rules

By using the Academy's IT facilities, you agree to comply with applicable laws, including these guidelines and regulations, and you agree that you will use our IT systems in a professional, responsible, and considerate manner - and only for educational purposes.

All users are responsible for any use of their personal rights and accounts. All users have a duty to handle passwords etc. responsibly, so that they do not inadvertently come into the hands of others.

Users may not damage, remove or change labels (e.g., PC name, model number, serial number, barcodes) on the Academy's IT equipment.

The Ten Commandments for Secure IT Use

You must follow the Ten Commandments for all use of IT equipment and the Internet via the Academy's network, as viruses, hacking or malicious software can have serious consequences for the network and risk affecting the entire operation of the Academy.

1. Never open ‘suspicious’ files, i.e., files where you are unsure what it is or who the sender is.

2. Never reply to/ or click on links in phishing emails (emails aimed at stealing your passwords, account information, etc.).

3. Use secure passwords, i.e., with both uppercase and lowercase letters, as well as numbers and preferably special characters – and never give them to others.

4. Protect all your ‘devices’ (including tablets, mobile phones, etc.) with password and/or PIN/fingerprint, and do not reuse passwords.

5. Prevent others from using your equipment by always locking your computer (e.g., via Windows + L or Control + Shift + Power on a Mac) when you leave it.

6. Be critical when installing apps on your phone or tablet and software on your computer.

7. Keep your PC up to date and always remember to have an up-to-date antivirus program installed on it. If in doubt, you can contact the IT ServiceDesk for guidance. If you suspect that your computer has been infected with a virus, report it to Servicedesk immediately.

8. Always use your Academy email when communicating with Business Academy Aarhus. We only use your Academy email or e-Boks when we need to contact you.

9. Don't access porn or gambling sites. Searching on such pages might be illegal, and there are often hidden viruses, spyware and destructive programs.

10. Remember to report security incidents to the IT Service Desk or your lecturer - even if you only suspect that unauthorised people have access to your account or IT equipment.

Unacceptable use of IT facilities and monitoring

Unacceptable use of the Academy's IT facilities means use that:

- is outright illegal
- compromises IT security
- creates disruptions with IT services due to policy/guideline breaches.

Below are several examples of activities that are not allowed when using the Academy's Internet access:

- Use of Internet access for private commercial purposes
- Using another user's password
- Search for information about password or data belonging to other users
- Activities that do not comply with applicable laws, including unauthorised copying of copyrighted material, use of unlicensed software, or dissemination of unauthorised copies of licensed software to others
- Attempts to intercept or examine data without the requisite rights or authorisation.

Please note that all movements on the Internet leave electronic traces and can be tracked. In many places you can choose the use of only necessary cookies. If possible, use the least number of cookies.

If you use the Academy's equipment/network, the electronic tracks can be attributed to Business Academy Aarhus (and subsequently to you).

Therefore, when you surf on the Internet from the Academy's network, you should never visit pages or take actions that in any way may be compromising for the Academy.

Managing user accounts

Students are created as users on the Academy's IT systems based on user data, which is created by the Academy's student administration department. Username, password, and your email address are stated in your user declaration as well as information on how the user must change their password.

At the end of your educational programme, the student's user account will be deactivated on the first day after the end of the programme. 90 days later, the student's user account and associated data will be deleted.

Users' access to the IT facilities is controlled through the granting of user rights, primarily based on information from the student administration system.

A user's access to our IT facilities will be closed if:

- The user is no longer a student
- The user has a longer leave of absence
- There are other justified circumstances in which management considers that access should be closed.

Access to users' personal email accounts, data, and documents

If there are operational issues, IT staff may need to open a student's email account without prior notice to rectify the problem. The owner of the email account will be informed of this as soon as possible and be given instructions on the correct use of the system.

When working with operational issues, IT employees may need to access data and files in connection with maintenance or investigation.

IT employees are subject to confidentiality in connection with access to email accounts, the personal data and the files just mentioned.

Monitoring and logging of IT systems

Monitoring and logging of our IT systems is done solely for the sake of operation, debugging, security, restoration, marketing, and documentation. This may be in connection with the investigation of IT facilities' log files for errors and/or operational disruptions, network monitoring, investigation of e-mails that have not been delivered to a mailbox, handling of virus and spam filters, use of the Internet, clarification of resource limitations, disclosure of information cases, etc.

As the Academy must be able to comply with a number of legislative requirements in relation to, among other things, the EU General Data Protection Regulation, the Criminal Code, and the Administrative and Public Administration Act, the Academy must weigh a number of factors:

On the one hand, the Academy must, on an equal footing with other public institutions, be able to manage disclosure of information cases in relation to the EU General Data Protection Regulation and disclosure of information in relation to the Administrative and Public Administration Act.

On the other hand, the Academy is equally interested in not violating our students' right to privacy. So, if you do send or receive privately related content in your Academy email (Outlook), you should move all your emails with privately related content into a ‘Private’ folder. You should do the same with private content on your OneDrive and H drive.

Access to logging and monitoring is limited to personnel whose job is to ensure IT operations. Thus, management only has access to data from logging/monitoring in cases of suspicion of abuse or crime.

IT employees and possibly external IT consultants respect confidentiality and have a duty of confidentiality in connection with access to users' email accounts, personal and possibly private data and files, and process this information in accordance with the provisions of the Personal Data Act.

Video surveillance

The Academy has video surveillance in selected areas such as entrances and certain corridors. The purpose is partly to create increased security for students and staff by preventing crime such as theft, assault, violence etc., and partly to improve the possibility of solving crimes.

All footage from the video surveillance is stored in a safe and secure manner and will only be reviewed in case of a crime. The recordings may not be published, disclosed, or presented to anyone other than the police. The recordings are automatically deleted after ten working days unless there is a reasonable suspicion of criminal offences.

Use of equipment, including the installation of programs

The Academy's AV equipment (e.g., Clevertouch screens and Airtame), printers, and PCs for borrowing are configured for our network and are automatically maintained over the network, including the security updates for Windows, the Office suite, and other software.

For the sake of efficient and secure operation, only the IT department can change these settings, just as only the IT department may service and repair the Academy's equipment.

Abuse

If you suspect that your password has been misused or that others have become aware of it, the IT Service Desk must be informed immediately, they will then reset the password.

If the IT Service Desk suspects misuse of your account, your password will also be reset. In addition, the specific case will be reported as a security breach to the school's GDPR officer and you will be notified.

Change your password at: https://mobil.efif.dk/Login.aspx

Digital education is a shared responsibility

Bullying, harassment, violations, sharing of images without consent via social media, as well as all forms of hacking, ticket fraud and digital media trading are absolutely prohibited. Business Academy Aarhus has focuses on ensuring that students can behave safely and morally in all situations, and it is important that they take care of themselves. Please be careful about requests from unknown people any any questionable links.

It is a criminal act to share other people's pictures/videos if they have not given consent - and of course this also applies to images/videos of a sexual nature.

Using borrowed PCs

As a rule, you must bring your own PC. However, on special occasions it is possible to borrow PCs from the Academy. Users are not allowed to change program and system settings on the PCs. The IT department will routinely download and update applications on the computers to ensure their full functionality. Any data on the computer's hard drive will be deleted. If you need to save your data, you must do this on your personal drive, in a cloud or on a USB memory stick. When you are finished working with a computer, you must log-out and turn off the computer.

Theft

Please note keeping your computer safe is your responsibility. Don't leave your computer unattended. The Academy is not responsible for theft of computers on Academy property.

Email

You will be assigned an Academy email address when you start on your programme. Emails are considered as personal, and you may not open someone else's email without their consent.

Never reply to spam mail or phishing mail.

All correspondence that is not marked as private in the subject line or that is not in a 'Private' folder is formally considered the property of the Academy, therefore others can, in principle, access and read them.

You should not use your Academy email for private use (e.g., in connection with social media - e.g., Facebook, chatting, discussion forums and newsgroups on the Internet, as well as completely private recipients). This is partly because the sender address is associated with Business Academy Aarhus, and partly because the risk of getting spam emails and security attacks increase as the e-mail address is disclosed to parties you do not know.

With unacceptable use of IT facilities

In cases where it is found that the Academy's IT policy has been violated, or where there is a reasonable suspicion of violation, the IT Manager will be contacted.

The IT manager will be responsible for all further developments.

In many cases, a conversation to clarify any incident with the parties involved will be sufficient. These could be misunderstandings, technical errors, or user errors and thus violations in which the user has quite unintentionally violated the rules.

If there are intentional violations of the Academy's IT policy (and not simple mistakes), the suspect, their head of programme and the rector/prorector will be involved in the investigation together with the IT manager.

Illegal use of the Academy's IT facilities (including the internet) may result in a reprimand, or a written warning and may also have disciplinary consequences such as expulsion for shorter or longer periods or permanently, and in extreme cases you will be reported to the police.

Legislation

Legislation related to the IT policy:

- Data Protection Act
- Public Administration Act
- Public Records Act
- Copyright Act
- The TV Surveillance Act.

January 2022

Hanne Troels Jensen
Head of Research and IT